# আর্থিক প্রতিষ্ঠানে তথ্য ও যোগাযোগ প্রযুক্তি

আবুল কাশেম মোঃ শিরিন

ব্যবস্থাপনা পরিচালক ও প্রধান নির্বাহী কর্মকর্তা
ডাচ্-বাংলা ব্যাংক লিমিটেড

উৎস প্রকাশন

প্রকাশনার চব্বিশ বছর
উৎস প্রকাশন



প্রকাশকাল
মে ২০২৪

প্রকাশক
মোস্তফা সেলিম
উৎস প্রকাশন
১২৭ আজিজ সুপার মার্কেট (৩য় তলা), শাহবাগ, ঢাকা-১০০০
ফোন : +৮৮০২৯৬৭৬০২৫, ০১৭১৫৪০৪১৩৪, ০১৭১৫৪৯৮৭৯৩৫
e-mail. utsopro2001@gmail.com

প্রচ্ছদ
মোস্তাফিজ কারিগর

মুদ্রণ
সানজানা প্রিন্টার্স, ৮১/১ নয়াপল্টন, ঢাকা-১০০০

দাম : ২৫০ টাকা

Aarthik Prothistane Totto O Jugajuk Poddothi by Abul Khashem Md Shirin Published by Mustafa Salim of Utso Prokashan 127 Aziz super market (2nd floor), Shahbagh, Dhaka 1000

ISBN : 978-984-98454-9-2

# মুখবন্ধ

দি ইনস্টিটিউট অব ব্যাংকার্স, বাংলাদেশ (আইবিবি) ১৯৭৩ সালে সোসাইটিজ রেজিস্ট্রেশন অ্যাক্ট এর আওতায় প্রতিষ্ঠিত হয়। প্রতিষ্ঠার পর থেকে আইবিবি দেশের ব্যাংক ও আর্থিক প্রতিষ্ঠানে কর্মরত কর্মকর্তা/কর্মচারীদের ব্যাংকিং প্রফেশনাল পরীক্ষা (জেএআইবিবি এবং এআইবিবি) গ্রহণের মাধ্যমে ব্যাংকিং জ্ঞানের পরিধি ও দক্ষতা বৃদ্ধিতে নিরলসভাবে কাজ করে যাচ্ছে। ব্যাংকিং প্রফেশনাল পরীক্ষা সাধারণত বছরে দুইবার বিভাগীয় শহরগুলোতে একযোগে অনুষ্ঠিত হয়। পরিবর্তনশীল অর্থনৈতিক অবস্থা, ব্যাংক ব্যবস্থা ও ব্যাংকিং পেশার সাথে সম্পর্কিত বিষয়গুলো বিবেচনা করে প্রণীত সিলেবাসের আওতায় ব্যাংকিং প্রফেশনাল পরীক্ষা পরিচালিত হয়।

যেহেতু ব্যাংকিং একটি ক্রমবর্ধমান পদ্ধতিগত প্রক্রিয়া, তাই ব্যাংকিং প্রফেশনাল পরীক্ষার সিলেবাসও পরিবর্তনশীল ব্যাংকিং ব্যবস্থার সাথে সঙ্গতিপূর্ণ হওয়া প্রয়োজন। এই উদ্দেশ্যে বিআইবিএম এর সাবেক মহাপরিচালক ড. তৌফিক আহমদ চৌধুরীর নেতৃত্বে জনাব মোঃ আলী হোসেন প্রধানিয়া, বাংলাদেশ কৃষি ব্যাংকের সাবেক ব্যবস্থাপনা পরিচালক; জনাব আবুল কাশেম মোঃ শিরিন, ডাচ্-বাংলা ব্যাংক পিএলসি'র ব্যবস্থাপনা পরিচালক ও প্রধান নির্বাহী কর্মকতা; ড. মোহাম্মদ হায়দার আলী মিয়া, সাবেক ব্যবস্থাপনা পরিচালক ও প্রধান নির্বাহী কর্মকতা, এক্সিম ব্যাংক অব বাংলাদেশ লিমিটেড; ড. শাহ মোঃ আহসান হাবীব, অধ্যাপক, বিআইবিএম; জনাব আলমগীর মোরশেদ, প্রধান নির্বাহী কর্মকর্তা, ইডকল; জনাব ওমর ফারুক, সিএফসিসি প্রধান, স্ট্যান্ডার্ড চার্টার্ড ব্যাংক এবং লাইলা বিলকিস আরা, মহাসচিব, আইবিবি এর সমন্বয়ে ব্যাংকিং প্রফেশনাল পরীক্ষার পাঠ্যক্রম হালনাগাদ করার উদ্দেশ্যে একটি কমিটি গঠন করা হয়। কমিটি দীর্ঘদিন পরিশ্রম করে এবং বেশ কয়েকটি সভায় মিলিত হয়ে ব্যাংকিং প্রফেশনাল পরীক্ষার (জেএআইবিবি এবং এআইবিবি) নতুন সিলেবাস প্রণয়ন করে যা কাউন্সিল কর্তৃক অনুমোদিত হয়।

আইবিবি'র ব্যাংকিং প্রফেশনাল পরীক্ষার সিলেবাসভুক্ত বিষয়গুলোর মানসম্পন্ন বই বা পঠন সামগ্রীর অভাবে পরীক্ষার্থীদের প্রস্তুতি গ্রহণ ছিল কষ্টসাধ্য। যে কারণে সকলের প্রত্যাশা ছিল ভালো মানের বই বা পঠন সামগ্রী পাওয়ার। তাই পরীক্ষার্থীদের জন্য মানসম্পন্ন বই বা পঠন সামগ্রী প্রণয়নের লক্ষ্যে সিলেবাস প্রস্তুতকরণ কমিটির সদস্যদেরকে অন্তর্ভুক্ত করে একটি রিডিং ম্যাটেরিয়াল প্রণয়ন কমিটি গঠন করা হয়। উক্ত কমিটি দেশের প্রথিতযশা ব্যাংকার এবং বিষয় বিশেষজ্ঞদেরকে বই লেখার জন্য নির্বাচন করেন।

আর্থিক প্রতিষ্ঠানগুলোতে তথ্য ও যোগাযোগ প্রযুক্তি (আইসিটিএফআই) বিষয়ের বইটি জনাব আবুল কাশেম মোঃ শিরিন কর্তৃক প্রথমে ইংরেজিতে প্রণয়ন করা হয়েছে। পরীক্ষার্থীদের চাহিদানুসারে বাংলায় অনুবাদকৃত বইটিও সুপঠনীয় হয়েছে যা পরীক্ষার্থীদের উপকারে আসবে। পাঠ্য সূচি অনুসারে বইটি লেখা অত্যন্ত দুরূহ ও কষ্টসাধ্য হওয়া সত্ত্বেও তিনি সাগ্রহে কাজটি করেছেন। এ কারণে আমরা তাঁকে আমাদের কৃতজ্ঞতা ও ধন্যবাদ জানাই।

সিলেবাসভুক্ত বিষয়গুলোর বই বা পঠন সামগ্রী ইতোমধ্যে ইংরেজিতে প্রণয়ন করে আইবিবি'র লার্নিং পোর্টালে আপলোড করা হয়েছে। পরবর্তীতে অন্যান্য বই/রিডিং ম্যাটেরিয়াল বাংলায় অনুবাদ করা হলে তা যথাসময়ে আইবিবি'র ই-লাইব্রেরি ওয়েব পোর্টালে প্রকাশ করা হবে। পরীক্ষার্থী, পাঠক, ব্যবহারকারীদেরকে যেকোনো পঠন সামগ্রীর বিষয়ে তাঁদের সুচিন্তিত মতামত পাঠাতে অনুরোধ করা হচ্ছে। পাঠকদের সুচিন্তিত মতামতকে গুরুত্ব সহকারে বিবেচনা করা হবে। এছাড়াও আইবিবি আগামীতে পরীক্ষার্থীদের সুবিধার্থে সময়ে সময়ে পঠন বিষয়গুলো পরিমার্জন ও পরিবর্তন করবে।

পরিশেষে, দি ইনস্টিটিউট অব ব্যাংকার্স, বাংলাদেশ (আইবিবি) ব্যাংকিং প্রফেশনাল পরীক্ষার পাঠ্যক্রম ও পাঠ্য উপকরণ প্রণয়ন করার জন্য আইবিবি কাউন্সিলের বিজ্ঞ সদস্য, সিলেবাস ও পরীক্ষা কমিটি ও রিডিং ম্যাটেরিয়াল প্রণয়ন কমিটির প্রতি কৃতজ্ঞতা প্রকাশ করছে।

লাইলা বিলকিস আরা
মহাসচিব

# সূচিপত্র

৩. মোবাইল আর্থিক পরিষেবা

৪. এজেন্ট ব্যাংকিং

৫. ই-কমার্স এবং এম-কমার্স
- ৫.১. ই-কমার্স
- ৫.২. এম-কমার্স

৬. কম্পিউটার হার্ডওয়্যার
- ৬.১. কম্পিউটারের বিকাশের ইতিহাস
- ৬.২. কম্পিউটারের প্রজন্ম
- ৬.৩. কম্পিউটারের প্রকারভেদ
- ৬.৪. কম্পিউটার হার্ডওয়্যার এবং ডিভাইস
  - ৬.৪.১. ইনপুট ডিভাইস (Input Device)
  - ৬.৪.২. আউটপুট ডিভাইস (Output Device)
  - ৬.৪.৩. প্রসেসিং ডিভাইস (Processing Device)
  - ৬.৪.৪. মেমরি ডিভাইস (Memory Device)
    - ৬.৪.৪.১. প্রাইমারি বা প্রধান মেমোরি
    - ৬.৪.৪.২. সেকেন্ডারি বা অক্সিলিয়ারি মেমোরি
    - ৬.৪.৪.৩. ক্যাশ মেমোরি (Cache Memory)
  - ৬.৪.৫. স্পেশাল বা বিশেষ ডিভাইস

৭. কম্পিউটার সফটওয়্যার
- ৭.১. সিস্টেম সফটওয়্যার
- ৭.২. অ্যাপ্লিকেশন সফটওয়্যার
- ৭.৩. প্রোগ্রামিং ভাষা (Programming Language)
  - ৭.৩.১. লো-লেভেল ভাষা (Low-level Language)
  - ৭.৩.২. হাই-লেভেল ভাষা (High-level Language)
  - ৭.৩.৩. অবজেক্ট ওরিয়েন্টেড ভাষা (Object Oriented Language)
- ৭.৪. ডাটাবেস ম্যানেজমেন্ট সিস্টেম (Database Management System)

৮. ইন্টারনেট এবং এর সম্পর্কিত পরিভাষা
- ৮.১. ইন্টারনেট (Internet)
- ৮.২. ডাব্লুউডাব্লুউডাব্লুউ (WWW)
- ৮.৩. হাইপারটেক্সট (Hypertext)
- ৮.৪. হাইপারলিঙ্ক (Hyper links)
- ৮.৫. ওয়েব ব্রাউজার (Web Browser)
- ৮.৬. ওয়েব পেজ (Web Page)
- ৮.৭. ইন্টারনেট বনাম ডাব্লিউডাব্লিউডাব্লিউ (Internet vs WWW)
- ৮.৮. ইউআরএল (URL)
- ৮.৯. ই-মেইল (e-mail)

**মডিউল-বি : আর্থিক প্রতিষ্ঠানের (FI) স্বয়ংক্রিয়করণের বিভিন্ন পদ্ধতি**

১. ডেটা সেন্টার (ডিসি), নিয়ার ডিসি, ডিজাস্টার রিকভারি সাইট (ডিআরএস), ডেটা সেন্টার স্ট্যান্ডার্ড ও সার্টিফিকেশন
- ১.১. ডেটা সেন্টার (DC)
- ১.২. নিয়ার ডিসি (Near DC)
- ১.৩. ডিজাস্টার রিকভারি সাইট (DRS)
- ১.৪. ডেটা সেন্টার স্ট্যান্ডার্ড ও সার্টিফিকেশন

২. কম্পিউটার নেটওয়ার্কিং
- ২.১. ল্যান ও ওয়ান-এর ধারণা
  - ২.১.১. লোকাল এরিয়া নেটওয়ার্ক (LAN)
  - ২.১.২. ওয়াইড এরিয়া নেটওয়ার্ক (WAN)
  - ২.১.৩. ট্রান্সমিশন মিডিয়া (Transmission Media)
    - ২.১.৩.১. ল্যানের জন্য ট্রান্সমিশন মিডিয়া
    - ২.১.৩.২. ওয়ান-এর জন্য ট্রান্সমিশন মিডিয়া
  - ২.১.৪ ব্যাংকের জন্য ল্যান/ওয়্যান
    - ২.১.৪.১. ফায়ারওয়াল (Firewall)
    - ২.১.৪.২. ডিএমজেড (DMZ)

৩. আইটি সিস্টেম, স্টোরেজ এবং ডাটাবেস ব্যাকআপ সিস্টেম
- ৩.১. আইটি সিস্টেম এবং স্টোরেজ
  - ৩.১.১. কম্পিউটার সার্ভার এবং প্রকার
  - ৩.১.২. রেইড (RAID)
  - ৩.১.৩. ক্লাস্টারিং (Clustering)
  - ৩.১.৪. রেপ্লিকেশন (Replication)
  - ৩.১.৫. ডার্ক ফাইবার (Dark Fiber)

৩.১.৬. বাহ্যিক স্টোরেজ সিস্টেম (External Storage System)
৩.১.৭. স্যান সুইচ (SAN Switch)
৩.২. ডাটাবেস ব্যাকআপ সিস্টেম (Database Backup System)

৪. এফআই (FI) কম্পিউটারাইজেশন পদ্ধতি
৪.১. স্ট্যান্ড-অ্যালোন সিস্টেম (Stand-alone System)
৪.২. ল্যান-ভিত্তিক সিস্টেম (LAN-based System)
৪.৩. ডিস্ট্রিবিউটেড ডাটাবেসসহ ওয়ান-ভিত্তিক সিস্টেম
৪.৪. কেন্দ্রীভূত ডাটাবেসসহ ওয়ান-ভিত্তিক সিস্টেম

**৫.** এফআই (FI) -এর জন্য বিভিন্ন সফ্টওয়্যার সিস্টেম
৫.১. কোর ব্যাংকিং সফটওয়্যার
৫.২. সফ্টওয়্যার সুইচিং
৫.৩. ক্রেডিট কার্ড সফটওয়্যার
৫.৪. পেমেন্ট গেটওয়ে সফটওয়্যার
৫.৫. মোবাইল ফিন্যান্সিয়াল সার্ভিসের জন্য সফটওয়্যার
৫.৫.১. এমএফএস বনাম কোর ব্যাংকিং সিস্টেম
৫.৫.২. এমএফএস বনাম এসএমএস ব্যাংকিং সিস্টেম
৫.৫.৩. মোবাইল ফিনান্সিয়াল সার্ভিসের (MFS) জন্য সহজলভ্য সফ্টওয়্যার
৫.৫.৪. এমএফএস-এর গ্রাহক এবং তাদের জন্য মেনু আইটেম
৫.৫.৫. মোবাইল ফিনান্সিয়াল সার্ভিসের (এমএফএস) জন্য সফটওয়্যারের বৈশিষ্ট্য
৫.৬. এজেন্ট ব্যাংকিং-এর জন্য সফট্ওয়্যার
৫.৬.১. এজেন্ট ব্যাংকিং সিস্টেমের জন্য সফট্ওয়্যার
৫.৬.২. এজেন্ট ব্যাংকিং সিস্টেম বনাম কোর ব্যাংকিং সিস্টেম
৫.৬.৩. এজেন্ট ব্যাংকিং সিস্টেম বনাম মোবাইল ব্যাংকিং সিস্টেম
৫.৬.৪. এজেন্ট ব্যাংকিং সিস্টেম-এ ব্যবহৃত ডিভাইসের প্রকারভেদ
৫.৬.৫. নিরাপত্তা (Security)
৫.৬.৬. এজেন্ট ব্যাংকিং সিস্টেমের জন্য প্রাপ্ত সফ্টওয়্যার
৫.৬.৭. এজেন্ট ব্যাংকিংয়ের গ্রাহক এবং তাদের জন্য মেনু আইটেম
৫.৬.৮. এজেন্ট ব্যাংকিং সেবার জন্য ব্যবহৃত সফট্ওয়্যারের বৈশিষ্ট্য

**মডিউল-সি : অল্টারনেটিভ ডেলিভারি চ্যানেল এবং ফান্ড ট্রান্সফার সিস্টেম**

১. অটোমেটেড টেলার মেশিন (ATM) এবং ক্যাশ রিসাইক্লিং মেশিন (CRM)
১.১. এটিএম/সিআরএম থেকে প্রাপ্ত পরিষেবা
১.২. অর্থ/নগদ তোলার ক্ষেত্রে এটিএম/সিআরএম কীভাবে কাজ করে?
১.৩. এটিএম/সিআরএম স্পেসিফিকেশন এবং এ সম্পর্কিত বিষয়াবলি
১.৩.১. এটিএম/সিআরএম স্পেসিফিকেশন
১.৩.২. এটিএম/সিআরএম-এ ব্যবহৃত নোটের মূল্যমান
১.৩.৩. ৩য় পক্ষের দ্বারা ক্যাশ ফিডিং
১.৩.৪. ক্যাশের পার্সিয়াল ডিসপেন্চ (Partial Dispense) ও নন-ডিসপেন্চ (Non-dispense)
১.৩.৫. টাকা ক্যাপচার (Capture of Money)
১.৩.৬. সংযোগের জন্য ব্যবহৃত নেটওয়ার্ক
১.৩.৭. কার্ড ক্যাপচার (Card Capture) এবং হট কার্ড (Hot Card)
১.৩.৮. এটিএম/সিআরএম বুথের জন্য এককালীন এবং মাসিক খরচ
১.৩.১০. এটিএম/সিআরএম থেকে আয়
১.৪. এটিএম/সিআরএম জালিয়াতি ও প্রতিকার (ATM/CRM Fraud and remedy)
১.৪.১. কার্ড রিডিং ডিভাইস (Card-Reading Device)
১.৪.২. কার্ড-ট্র্যাপিং ডিভাইস (Card-Trapping Device)

১২. তহবিল স্থানান্তর নির্দেশ পাঠানোর জন্য সিস্টেমসমূহ
- ১২.১. টেলেক্স (Telex)
- ১২.২. সুইফট (SWIFT)
  - ১২.২.১. সুইফট কী?
  - ১২.২.২. সুইফট ট্রাফিক
  - ১২.২.৩. সুইফট সদস্যপদ
  - ১২.২.৪. কেন সুইফট সদস্য হতে হবে?
  - ১২.২.৫. সুইফট এ নিরাপত্তা
  - ১২.২.৬. সুইফট কীভাবে কাজ করে?
  - ১২.২.৭. সুইফটের সমস্যাগুলো কী?
  - ১২.২.৮. বাংলাদেশে ব্যবহারকারী গ্রুপ
- ১২.৩. বাংলাদেশ অটোমেটেড ক্লিয়ারিং হাউস (BACH)
  - ১২.৩.১. বাংলাদেশ অটোমেটেড চেক প্রসেসিং সিস্টেম (BACPS)
  - ১২.৩.২. বাংলাদেশ ইলেকট্রনিক ফান্ড ট্রান্সফার নেটওয়ার্ক (BEFTN)
- ১২.৪. এনপিএসবি (NPSB)
- ১২.৫. আরটিজিএস (RTGS)
- ১২.৬. চিপস (CHIPS)
- ১২.৭. ফেডওয়্যার (FEDWIRE)

**মডিউল ডি : আইসিটি সিকিউরিটি, সাইবার সিকিউরিটি, আইসিটি রিস্ক ম্যানেজমেন্ট, স্ট্যান্ডার্ড, রেগুলেশনস এবং লিগ্যাল ফ্রেমওয়ার্ক**

১. আইসিটি নিরাপত্তা (ICT Security)
- ১.১. ব্যবসার ধারাবাহিকতা হুমকি (Business Continuty Threats)
- ১.২. অভ্যন্তরীণ হুমকি (Internal Threats)
- ১.৩. মোবাইল ফিন্যান্সিয়াল সার্ভিসেস (MFS) সম্পর্কিত ঝুঁকি
- ১.৪. এটিএম/পিওএস/ই-কম/কার্ড সম্পর্কিত হুমকি
  - ১.৪.১ এটিএম স্কিমিং (ATM Skimming)
  - ১.৪.২. পিওএস স্কিমিং (POS Skimming)
  - ১.৪.৩. এটিএম জ্যাকপটিং (ATM Jackpotting)
  - ১.৪.৪. ই-কমার্স জালিয়াতি (e-commerce fraud)
- ১.৫. বাহ্যিক ঝুঁকি (External Risks)/ সাইবার হুমকি (Cyber Threats)
  - ১.৫.১. ডিস্ট্রিবিউটেড ডিনায়াল অব সার্ভিস (DDOS)
  - ১.৫.২. র‍্যানসমওয়্যার (Ransomware)
  - ১.৫.৩. ম্যালওয়্যার (Malware)
- ১.৬. হ্যাকিং এবং অননুমোদিত অর্থ স্থানান্তর (Hacking and Unauthorized Transfer of Money)
- ১.৭. ক্রেডিট কার্ডের ডেটা চুরি করা (Stealing of Credit Card Data)
- ১.৮. ক্রিপ্টো মুদ্রার হুমকি (Crypto Currency Threats)
- ১.৯. ঝুঁকি কমাতে কী করতে হবে?

২. সাইবার নিরাপত্তা (Cyber Security)

৩. আইসিটি ঝুঁকি ব্যবস্থাপনা (ICT Risk Management)

৪. নিরাপত্তা স্ট্যান্ডার্ড এবং প্রবিধান (Security Standards and Regulations)

৫. বাংলাদেশ কেন্দ্রীয় ব্যাংক দ্বারা প্রকাশিত তফসিলি ব্যাংক এবং আর্থিক প্রতিষ্ঠানের জন্য আইসিটি নিরাপত্তা সংক্রান্ত নির্দেশিকা (২০১৫)
- ৫.১. ব্যাংক ও এনবিএফআই-এর শ্রেণিকরণ
- ৫.২. আইসিটি নিরাপত্তা ব্যবস্থাপনা
  - ৫.২.১. ভূমিকা ও দায়িত্ব
  - ৫.২.২ আইসিটি নীতি, মান ও পদ্ধতি
  - ৫.২.৩ ডকুমেন্টেশন
  - ৫.২.৪ অভ্যন্তরীণ তথ্য সিস্টেম নিরীক্ষা
  - ৫.২.৫ বাহ্যিক তথ্য সিস্টেম নিরীক্ষা
  - ৫.২.৬ স্ট্যান্ডার্ড সার্টিফিকেশন
  - ৫.২.৭ নিরাপত্তা সচেতনতা ও প্রশিক্ষণ
  - ৫.২.৮ বীমা বা ঝুঁকি কভারেজ ফান্ড
- ৫.৩. আইসিটি ঝুঁকি ব্যবস্থাপনা
  - ৫.৩.১ আইসিটি ঝুঁকি নিয়ন্ত্রণ
  - ৫.৩.২ আইসিটি ঝুঁকি মূল্যায়ন
  - ৫.৩.৩ আইসিটি ঝুঁকি প্রতিক্রিয়া
- ৫.৪. আইসিটি সার্ভিস ডেলিভারি ম্যানেজমেন্ট
  - ৫.৪.১ পরিবর্তন ব্যবস্থাপনা (Change Management)
  - ৫.৪.২. ঘটনা ব্যবস্থাপনা (Incident Management)
  - ৫.৪.৩ সমস্যা ব্যবস্থাপনা (Problem Management)

৬.৩.১. আইএসএমএস (ISMS) বাস্তবায়নের সুবিধা
৬.৩.২. আইএসও ২৭০০১ এর ১৪টি ডোমেইন কী কী?
৬.৩.৩. আইএসও ২৭০০১ এ কয়টি নিয়ন্ত্রণ আছে?
৬.৩.৪. 'আইএসও ২৭০০১ প্রত্যয়িত' বলতে কী বোঝায়?

৭. বাংলাদেশে আইনি কাঠামো
৭.১. সাইবার আইন (Cyber Law)
৭.১.১. সাইবার আইন কী?
৭.১.২. সাইবার অপরাধ শ্রেণিকরণ
৭.১.৩. সাইবার অপরাধ কার্যক্রম
৭.২. আইসিটি আইন (ICT Act)
৭.২.১. ভূমিকা
৭.২.২. আইসিটি আইন-২০০৬ এর প্রযোজ্য ফিল্ডসমূহ
৭.২.৩. অবজেক্টিভ
৭.২.৪. নির্বাচিত ধারাসমূহ

**মডিউল-ই: ডকুমেন্ট হ্যান্ডলিং সিস্টেম, অতিরিক্ত ব্যাংকিং অ্যাপ্লিকেশন এবং অন্যান্য দিক**

১. চেক প্রসেসিং সিস্টেম
১.১. ক্লিয়ারিং এবং সেটেলমেন্ট সিস্টেম
১.২. প্রচলিত চেক ক্লিয়ারিং প্রক্রিয়া
১.৩. MICR (ম্যাগনেটিক ইঙ্ক ক্যারেক্টার রিকগনিশন)
১.৪. চেক ট্রাঙ্কেশন (Cheque truncation)
১.৫. RTGS (রিয়েল টাইম গ্রস সেটেলমেন্ট)
১.৬. BACH (বাংলাদেশ অটোমেটেড ক্লিয়ারিং হাউস)
১.৬.১. বাংলাদেশ অটোমেটেড চেক প্রসেসিং সিস্টেম (BACPS)
১.৬.২. বাংলাদেশ ইলেকট্রনিক ফান্ড ট্রান্সফার নেটওয়ার্ক (BEFTN)

২. অতিরিক্ত ব্যাংকিং অ্যাপ্লিকেশন
২.১. ইআরপি (ERP) সফটওয়্যার
২.১.১ ERP সিস্টেম কী?
২.১.২ একটি ERP সফ্টওয়্যারের কম্পোনেন্ট/মডিউল
২.১.৩ একটি ERP সিস্টেমের কম্পোনেন্ট
২.১.৪. ইআরপি সিস্টেমের সুবিধা ও অসুবিধা
২.১.৫. বিখ্যাত ইআরপি সফ্টওয়্যার:
২.১.৫.১. এসএপি-এর এসএপি ইআরপি (SAP ERP)
২.১.৫.২. ওরাকল-এর পিপলসফট ইআরপি (People Soft ERP)

২.২. সিআরএম (CRM) সফটওয়্যার
২.২.১. সিআরএম কী?
২.২.২. ব্যবহারের ক্ষেত্রসমূহ
২.২.২.১. সেলস ফোর্স অটোমেশন
২.২.২.২. মার্কেটিং
২.২.২.৩. গ্রাহক সেবা ও সাপোর্ট
২.২.২.৪ বিশ্লেষণ (Analysis)
২.২.২.৫. সমন্বিত/সহযোগী (Integrated/Collaborative)
২.২.৩. সিআরএম-এর জন্য সফটওয়্যার
২.৩. ই-মেইল সফটওয়্যার
২.৩.১. ই-মেইল কী?
২.৩.২. অপারেশন ওভারভিউ
২.৩.৩. একটি মেসেজিং সিস্টেমের উপাদান
২.৩.৪. জনপ্রিয় ই-মেইল সিস্টেম
২.৩.৪.১. সেন্ড মেইল (Sendmail)
২.৩.৪.২. কিউ মেইল (Qmail)
২.৩.৪.৩. মাইক্রোসফট এক্সচেঞ্জ সার্ভার (Microsoft Exchange Server)
২.৩.৪.৪. লোটাস ডমিনো (Lotus Domino)
২.৩.৫. বাণিজ্যিক পণ্যের লাইসেন্সিং
২.৩.৫.১. এক্সচেঞ্জ সার্ভার (Exchange Server)
২.৩.৫.২. লোটাস ডমিনো (Lotus Domino)
২.৪. অ্যান্টিভাইরাস সফটওয়্যার (Antivirus Software)
২.৪.১. অ্যান্টিভাইরাস সফটওয়্যার কী?
২.৪.২. অ্যান্টিভাইরাস কিভাবে কাজ করে?
২.৪.২.১. স্বাক্ষরভিত্তিক শনাক্তকরণ (Signature based detection)

২.৪.২.২. আচরণভিত্তিক শনাক্তকরণ (Behavior based detection)
২.৪.৩. লাইসেন্সিং (Licensing)
২.৪.৪. জনপ্রিয় অ্যান্টিভাইরাস প্রোগ্রাম
২.৫. অ্যান্টি-ম্যালওয়্যার সফ্টওয়্যার

**মডিউল-এফ: ফিনটেক, কৃত্রিম বুদ্ধিমত্তা এবং ভবিষ্যৎ প্রযুক্তিভিত্তিক ব্যাংকিং**

১. ফিনটেক, র‍্যাগটেক ও টেকফিন
১.১. ফিনটেক (FinTech)
১.২ টেকফিন (TechFin)
১.৩ র‍্যাগটেক (RegTech)

২. বেসিক ক্রিপ্টো কারেন্সি (Crypto Currency) এবং ব্লক চেইন প্রযুক্তি (Block Chain Technology)
২.১ ব্লক চেইন প্রযুক্তি (Block Chain Technology)
২.২ মৌলিক ক্রিপ্টো কারেন্সি
২.২.১. কেন ক্রিপ্টো-কারেন্সি?
২.২.২. সাতোশি নাকামোতো (Satashi Nakamoto) কে?
২.২.৩. বাংলাদেশে ক্রিপ্টো-কারেন্সি
২.২.৪. লিগ্যাল টেন্ডার কী?
২.২.৫. ক্রিপ্টো-কারেন্সির বর্তমান অবস্থা
২.২.৬. ক্রিপ্টো-কারেন্সি কীভাবে কাজ করে?
২.২.৭. সমাধান কী?
২.২.৮. জাতীয় ডিজিটাল মুদ্রার (NDC) পরিচিতি

৩. কৃত্রিম বুদ্ধিমত্তা (Artificial Intelligence)

৪. ভবিষ্যৎ প্রযুক্তি-ভিত্তিক ব্যাংকিং
৪.১ ভার্চুয়াল ব্যাংকিং (Virtual Banking)
৪.২ ক্লাউড কম্পিউটিং (Cloud Computing)
৪.৩ ইন্টারনেট অফ থিংস (IoT)
৪.৪ মেশিন লার্নিং (Machine Learning)
৪.৫ ডেটা মাইনিং (Data Mining)
৪.৬ ডেটা ওয়্যারহাউস (Data Warehouse)
৪.৭ সাম্প্রতিক প্রবণতা (Current trends)

আর্থিক প্রতিষ্ঠানে তথ্য ও যোগাযোগ প্রযুক্তি

মডিউল-এ

# আইসিটি ও কম্পিউটার সিস্টেমের ভূমিকা

## ১ তথ্য ও যোগাযোগ প্রযুক্তি (ICT)

### ১. ১.১. আইসিটি কী?

তথ্য এবং যোগাযোগ প্রযুক্তি (আইসিটি) হলো এমন একটি প্রযুক্তি যা কম্পিউটার সিস্টেম (যেমন কম্পিউটার হার্ডওয়্যার ও স্টোরেজ), সফ্টওয়্যার (যেমন অ্যাপ্লিকেশন ও ডাটাবেস) এবং তথ্যের যোগাযোগের জন্য ব্যবহৃত সিস্টেমগুলোকে বোঝায় (যেমন নেটওয়ার্কিং ডিভাইস ও প্রযুক্তি) যা একত্রিতভাবে ডিজিটাল বিশ্বে মানুষ ও প্রতিষ্ঠানগুলোকে যোগাযোগে সাহায্য করে।

### ১.২. কম্পিউটার কী?

সি.এস. ফ্রেঞ্চ প্রদত্ত সংজ্ঞা অনুসারে, একটি কম্পিউটার এমন একটি ডিভাইস যা ডেটা বা তথ্য গ্রহণ করতে পারে, ডেটা প্রক্রিয়াকরণ করতে পারে এবং ডেটা আউটপুট হিসাবে প্রদান করতে পারে। অন্য কথায়, একটি কম্পিউটার হলো

*ল্যাপটপ কম্পিউটার*

একটি মেশিন যা কিছু প্রোগ্রাম দ্বারা নিয়ন্ত্রিত হয়, ইনপুট হিসাবে ডেটা গ্রহণ করে, সেগুলো প্রক্রিয়া করে এবং অবশেষে ফলাফল বা প্রয়োজনীয় তথ্য আউটপুট হিসাবে ব্যবহারকারীদের কাছে প্রদর্শন করে। উদাহরণস্বরূপ, গ্রাহকরা ব্যাংকে টাকা জমা করে এবং ব্যাংক থেকে টাকা উত্তোলন করে। জমা বা তোলার পরিমাণ একটি ব্যাংক টেলার দ্বারা কম্পিউটারে ডেটা হিসাবে ঢোকানো হয়। এখন কম্পিউটার ডেটা প্রক্রিয়া করে, যার মধ্যে 'গ্রাহক লেজারে' গ্রাহকদের ব্যালেন্স আপডেট করা অন্তর্ভুক্ত। দিনের শেষে, কম্পিউটার 'ব্যালেন্স লিস্টিং' এবং 'স্টেটমেন্ট অব অ্যাফেয়ার্স' তৈরি করে, যাকে বলা হয় আউটপুট। আউটপুটের উপর ভিত্তি করে, ব্যবহারকারী ও ব্যবস্থাপনা কর্তৃপক্ষ গুরুত্বপূর্ণ সিদ্ধান্ত গ্রহণ করে।

তাছাড়া আজকাল কম্পিউটার অন্যান্য অনেক উপায়েও ব্যবহৃত হয় যেমন ই-মেইলিং, ব্রাউজিং, গেম খেলা, গান শোনা, ভিডিও এবং টিভি দেখা, ফোন কল করা ইত্যাদি।

### ১.৩. তথ্য প্রযুক্তি কী?

সংক্ষেপে, তথ্য প্রযুক্তি আইটি নামে পরিচিত। সি. এস. ফ্রেঞ্চের মতে, তথ্য প্রযুক্তি (আইটি) হচ্ছে এমন একটি প্রযুক্তি যা তথ্যের সৃষ্টি, সংরক্ষণ, নিয়ন্ত্রণ ও যোগাযোগের সঙ্গে জড়িত ক্রিয়াকলাপগুলো এবং এর সঙ্গে সম্পর্কিত পদ্ধতি, ব্যবস্থাপনা ও প্রয়োগ নিয়ে কাজ করে।

তথ্য প্রযুক্তি কেবল তথ্য প্রক্রিয়াকরণের মধ্যেই সীমাবদ্ধ নয়, তথ্যের যোগাযোগের সঙ্গেও কাজ করে, তাই এই শব্দটিকে তথ্য ও যোগাযোগ প্রযুক্তিও বলা হয়। তথ্য গ্রহণ, সংগ্রহ, প্রক্রিয়া ও যোগাযোগের জন্য প্রয়োজনীয় সমস্ত প্রক্রিয়া ও পদ্ধতিকে সমষ্টিগতভাবে তথ্য প্রযুক্তি বলা হয়।

### ১.৪. আইসিটি এর গুরুত্ব ও ব্যবহার

ব্যাংকিংয়ে তথ্য ও যোগাযোগ প্রযুক্তির (আইসিটি) ব্যবহার গ্রাহক সেবায় বৈপ্লবিক পরিবর্তন এনেছে। আইসিটির যে বৈশিষ্ট্যগুলোর জন্য এটি আর্থিক পরিষেবাগুলোতে অনেক অবদান রেখেছিল তা নিচে আলোচনা করা হয়েছে:

#### ক. উচ্চ গতি

কম্পিউটার খুব উচ্চ গতিতে কাজ করতে পারে। একটি কম্পিউটার মাত্র কয়েক মিনিটে একজন মানুষের ১০০ বছরের কাজ শেষ করতে পারে।

১৯৮০-এর দশকে বাংলাদেশে ব্যাংকিং খাতে কোনো আইসিটি ব্যবহার করা হতো না। সেই সময়, ব্যাংকাররা একটি ম্যানুয়াল লেজার বজায় রাখতেন। যখন

একজন গ্রাহক টাকা তোলার জন্য ব্যাংক কাউন্টারে আসতেন, প্রথমে টেলারকে ম্যানুয়ালি স্বাক্ষরটি পরীক্ষা করতে হতো এবং একটি বড় খাতায় টাকা তোলার তথ্যসমূহ এন্ট্রি করতে হয় এবং তারপরে গ্রাহকের কাছে টাকা হস্তান্তর করা হতো। এতে দীর্ঘ সময় লাগত এবং গ্রাহকদের ঘণ্টার পর ঘণ্টা লাইনে দাঁড়িয়ে থাকতে হতো। ব্যাংকগুলোতে আইসিটি প্রবর্তনের পর, কম্পিউটারভিত্তিক লেজারে পোস্টিং শুধু এক মিনিটের কার্যকলাপে পরিণত হয়েছে এবং দ্রুত গ্রাহক পরিষেবা প্রদান সম্ভব হচ্ছে। অন্যদিকে, দিন-শেষ, সপ্তাহ-শেষ, মাস-শেষ এবং বছরের শেষের ক্রিয়াকলাপ যেমন মুনাফার গণনা, আয়-ব্যয় গণনা, ট্রায়াল ব্যালেন্স, ব্যালেন্স শিট, Statement of Affairs এবং আয়-ব্যয় প্রতিবেদন তৈরি করা ব্যাংকারদের জন্য একটি দুঃসহ কাজ ছিল। তবে কম্পিউটারাইজেশনের পর কম্পিউটারের মাধ্যমে দ্রুত এসব কার্যক্রম সম্পন্ন হচ্ছে এবং ব্যাংকারদের দুর্ভোগ কমেছে। ফলে ব্যাংকাররা ব্যবসার উন্নয়নের অন্যান্য কর্মকাণ্ডে অনেক বেশি মনোযোগ দিতে সক্ষম হচ্ছেন।

**খ. যে কোনো সময় প্রাপ্তিসাধ্য**

ব্যাংকিং পরিষেবাগুলোতে আইসিটি প্রবর্তনের পূর্বে, গ্রাহককে শুধু কার্যদিবসের মধ্যে একটি নির্দিষ্ট সময়ের পূর্বে সমস্ত লেনদেন সম্পন্ন করতে হতো। এখন দিনে ২৪ ঘণ্টা, বছরে ৩৬৫ দিন ব্যাকিং পরিষেবা অবারিত। একজন গ্রাহক যে কোনো সময় টাকা তুলতে এটিএম ব্যবহার করতে পারেন। ব্যাংকের ডেটা সেন্টারের কম্পিউটারগুলো সর্বদা চলমান অবস্থায় থাকে এবং গ্রাহকদের ব্যালেন্স তাৎক্ষণিকভাবে আপডেট করতে পারে। অন্যদিকে ব্যাংকাররা যথাসময়ে সমস্ত কার্যকলাপ প্রতিবেদন (যেমন কে টাকা উত্তোলন করছে, পরিমাণ কত এবং কোথা থেকে উত্তোলন করছে ইত্যাদি) পেতে পারে। ইন্টারনেট ব্যাংকিং সিস্টেম ব্যবহার করে একজন গ্রাহক যেকোন সময় তার অফিস বা বাসা থেকে ব্যাংকিং করতে পারেন। গ্রাহকরা দোকান থেকে পণ্য ও পরিষেবা কিনতে পারেন এবং যে কোনো সময় তার ডেবিট বা ক্রেডিট কার্ড এবং দোকানে স্থাপিত পিওএস টার্মিনাল ব্যবহার করে অনলাইনে বিল পরিশোধ করতে পারেন। একজন গ্রাহকও তার মোবাইল ফোন ব্যবহার করে এবং যেকোনো সময় কিছু লেনদেন করতে পারেন।

**গ. যে কোনো জায়গায় পাওয়া যায়**

ব্যাংকিং পরিষেবাগুলোতে আইসিটি প্রবর্তনের পূর্বে, একজন গ্রাহককে ব্যাকিং পরিষেবাগুলো পাওয়ার জন্য শারীরিকভাবে একটি নির্ধারিত শাখায় যেতে হতো। এখন গ্রাহক তার ইচ্ছামতো যেকোনো জায়গা থেকে ব্যাংকিং সেবা নিতে পারেন। তিনি যে শাখায় অ্যাকাউন্ট খুলেছেন শুধু সেখানেই নয়, যে কোনো শাখা থেকে সম্পূর্ণ ব্যাকিং পরিষেবাগুলো পেতে পারেন। তিনি যেকোনো শহরের এটিএম-এ থেকে তুলতে পারেন, ব্যালেন্স চেক করতে পারবেন, মিনি স্টেটমেন্ট প্রিন্ট করতে পারবেন, টাকা জমা দিতে পারেন এবং ইউটিলিটি বিল পরিশোধ করতে পারেন। গ্রাহক বিশ্বের যেকোনো শহরের যেকোনো দোকানে গিয়ে তার আন্তর্জাতিক ক্রেডিট বা ডেবিট কার্ড ব্যবহার করে পণ্য ও সেবা কিনতে পারেন। তিনি বিশ্বের যেকোনো প্রান্ত থেকে মোবাইল অ্যাপ বা ইন্টারনেটের মাধ্যমে তার অ্যাকাউন্টে প্রবেশ করতে পারেন।

**ঘ. সঠিকতা/যথার্থতা**

কম্পিউটার (আইসিটির একটি উপাদান) ১০০% নির্ভুলতার সঙ্গে কাজ করতে পারে যদি প্রোগ্রাম ও সরবরাহকৃত ডেটা সঠিক হয়। 'গার্বেজ ইন গার্বেজ আউট' কম্পিউটারের জন্য খুব সত্য। কম্পিউটার কখনো ভুল করতে পারে না। যাহোক, ডেটা ভুল হলে বা প্রোগ্রামিং লজিক ভুল হলে এটি ভুল ফলাফল দিতে পারে। একজন গ্রাহক যদি টাকা উত্তোলন করেন ১০০/- টাকা এবং কম্পিউটারে পোস্ট করার সময় টেলার টাইপ করেন ১০০/- টাকার পরিবর্তে ১০০০/- টাকা, তাহলে গ্রাহকের ব্যালেন্স ভুলভাবে আপডেট হবে। এটি কম্পিউটারের ত্রুটি নয়, ভুলভাবে ডাটা প্রদান এর জন্য দায়ী।

**ঙ. মেমোরি**

একটি কম্পিউটারের বিশাল মেমোরি রয়েছে—এটি প্রচুর পরিমাণে ডেটা সংরক্ষণ ও প্রক্রিয়া করতে পারে। এর স্টোরেজ একটি বড় লাইব্রেরির স্টোরেজের চেয়েও বেশি। এটি গ্রাহকের কয়েক বছরের ডেটা সংরক্ষণ করতে পারে। কম্পিউটার খুব দ্রুত এবং নির্ভুলভাবে স্টোরেজ থেকে ডেটা পুনরুদ্ধার করতে পারে।

**চ. কর্মক্ষমতা**

কম্পিউটার ক্লান্তি ছাড়া একটানা দীর্ঘ সময় কাজ করতে পারে যা একজন মানুষের পক্ষে সম্ভব নয়। একটি ব্যাংকের একটি কম্পিউটার সার্ভার একবার চালু করা হয় এবং একসঙ্গে বছরের পর বছর চলতে থাকে। এভাবে এটিএম, পিওএস টার্মিনাল, ইন্টারনেট ব্যাকিং, ই-কমার্স ইত্যাদির মতো ব্যাকিং পণ্যগুলোর জন্য অবিরাম ২৪/৭ পরিষেবা সম্ভব।

**ছ. ইন্টারফেসিং**

ইন্টারফেসিং হলো একটি আইসিটি সিস্টেমের সঙ্গে অন্য আরেকটি সিস্টেমের যোগাযোগ করার উপায়, যেমন একটি ব্যাংকের আইসিটি সিস্টেম থেকে অন্য ব্যাংকের আইসিটি সিস্টেমের সঙ্গে যোগাযোগ করা। এভাবে মালয়েশিয়ার 'মে' ব্যাংকের একজন গ্রাহক তার ভিসা বা মাস্টারকার্ড ব্যবহার করে বাংলাদেশের ডাচ্-বাংলা ব্যাংকের এটিএম থেকে টাকা তুলতে পারবেন। অন্যদিকে, ডাচ্-বাংলা ব্যাংকের একজন গ্রাহক তার মাস্টারকার্ড বা ভিসা কার্ড ব্যবহার করে মার্কিন যুক্তরাষ্ট্রে একটি দোকানে কেনাকাটার বিল পরিশোধ করতে পারেন।

## ২. ইলেকট্রনিক ব্যাংকিং এবং অনলাইন ব্যাংকিং

### ২.১. ইলেকট্রনিক ব্যাংকিং

ইলেকট্রনিক ব্যাংকিং হলো একটি আধুনিক ব্যাংকিং কৌশল যা ব্যবহার করে একজন ব্যাংক গ্রাহক সশরীরে ব্যাংক শাখায় না গিয়ে এবং কোনও ব্যাংক কর্মকর্তার সাহায্য ছাড়াই ব্যাংকিং পরিষেবা পেতে পারেন। ইলেকট্রনিক ব্যাংকিং পরিষেবাগুলো নিচে বর্ণিত হয়েছে—

#### ২.১.১. এটিএম (ATM)

এটিএম বা স্বয়ংক্রিয় টেলার মেশিন মূলত ব্যাংক গ্রাহকের ডেবিট, ক্রেডিট বা প্রিপেইড কার্ড ব্যবহার করে নগদ টাকা তোলার জন্য ব্যবহৃত হয়। এছাড়াও এটিএম কার্ডধারক তার অ্যাকাউন্টের বর্তমান অবস্থার তথ্য পেতে (কাগজে একটি প্রিন্টসহ) এবং এক অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে অর্থ স্থানান্তর করতেও এটিএম ব্যবহার করা হয়।

এটিএম এর সঙ্গে সংযুক্ত থাকে কার্ডেও তথ্য পড়ার জন্য একটি ডিভাইস, একটি ডিসপ্লে মনিটর ও কার্ডধারকের সঙ্গে

*একটি অটোমেটেড টেলার মেশিন Machine*

যোগাযোগের জন্য একটি কীবোর্ড। এটিএম এর সঙ্গে ব্যক্তিগত কম্পিউটার থাকে যা পিন চেক করার জন্য, অ্যাকাউন্টের ব্যালেন্স আপডেট করার জন্য এবং অবশেষে নগদ টাকা বিতরণ করা যায় কি না তা জানার জন্য ব্যাংকের কেন্দ্রীয় সার্ভারের সঙ্গে যোগাযোগ করে।

ক্যাশ ডিস্পেন্সার নগদ অর্থের ভাণ্ডার। বিভিন্ন মানের টাকার নোট বিভিন্ন ক্যাসেটে রাখা হয় এবং ক্যাসেটসমূহ একটি ভল্টে স্থাপন করা হয়। ক্যাসেটের সংখ্যা একটি এটিএম কত ধরনের নোট প্রদান করতে পারে তা নির্ধারণ করে। এটিএম-এ একটি ল্যান কার্ড সংযুক্ত থাকে যাহা কেন্দ্রীয় সার্ভারের সঙ্গে যোগাযোগের জন্য ব্যবহৃত হয়।

বাংলাদেশের ব্যাংকগুলো গ্রাহকদের কাছে ব্যাংকিং সেবা পৌঁছে দেওয়ার লক্ষ্যে দেশের বিভিন্ন স্থানে এটিএম স্থাপন করেছে। তাই গ্রাহকদের টাকা তোলা বা অন্যান্য পরিষেবার জন্য ব্যাংকের শাখায় যেতে হয় না। গ্রাহক তার বাসভবন, অফিস বা দোকান/মার্কেটের কাছে স্থাপন করা যেকোনো এটিএম থেকে এই পরিষেবাগুলো পেতে পারেন। এটিএমগুলো দিনে ২৪ ঘণ্টা এবং বছরে ৩৬৫ দিন খোলা থাকে। এইভাবে, গ্রাহকরা ছুটির দিনেও সারা দিন এবং রাতে টাকা তুলতে বা জমা করতে পারবেন। এটি গ্রাহকদের ব্যাংকিং করার স্বাধীনতা দিয়েছে। এখন গ্রাহকরা বিকাল ৩টায় ক্যাশ কাউন্টার বন্ধ হওয়ার আগে অথবা একটি দীর্ঘ ছুটির আগে বা অন্য শহরে একটি যাত্রা করার আগে টাকা তোলা নিয়ে চিন্তিত নন। ব্যাংক গ্রাহকরা এটিএম নেটওয়ার্ক থেকে নিম্নলিখিত পরিষেবাগুলো পেতে পারেন—

*একটি কারখানা এটিএম তৈরি করছে। ভল্ট ও বিতরণ ইউনিট ছবিতে দেখা যাচ্ছে*

ক. নগদ উত্তোলন।
খ. ইউটিলিটি বিল প্রদান।
গ. গ্রাহকদের নিজস্ব একাউন্ট থেকে ফান্ড একই ব্যাংকের বা অন্য ব্যাংকের অন্য আরেকটি একাউন্টে স্থানান্তর করা।
ঘ. অ্যাকাউন্টের ব্যালেন্স চেক করা।
ঙ. মিনি স্টেটমেন্ট প্রিন্ট করা (শেষ ৫টি লেনদেন)।

এটিএম বুথ এমন একটি জায়গা যেখানে একটি ব্যাংক দ্বারা এক বা একাধিক এটিএম ইনস্টল করা হয়। কিছু এটিএম বুথে, ক্যাশ ডিপোজিট মেশিন (সিডিএম) স্থাপন করা হয়েছে, যেখানে খামে করে নগদ অর্থ বা চেক জমা দেওয়া যায়। এই ধরনের ক্ষেত্রে, গ্রাহক তার অ্যাকাউন্ট নম্বর ও ডিপোজিট মেশিনে জমা দেওয়ার পরিমাণ ইনপুট করে। মেশিনটি তার দরজা খুলে দেয় এবং গ্রাহক খামটি মেশিনে ফেলে দেয়। অর্থ জমা করার এই পদ্ধতিতে, ব্যাংকগুলো কখনও কখনও দেখতে পারে যে সিস্টেমে ইনপুট করা অংকের সঙ্গে খামে লিখিত অর্থের পরিমাণ মিলছে না। এতে বিরোধ তৈরি হতে পারে। ব্যাংক সাধারণত সিসিটিভি সিস্টেমের নজরদারির অধীনে খামের ভেতর থেকে প্রাপ্ত এই ধরনের অর্থ গণনা করে থাকে, এই ধরনের অসঙ্গতি রেকর্ড করতে।

এমন এটিএম মেশিন রয়েছে যা টাকা বান্ডিল আকারে গ্রহণ করতে পারে, বিভিন্ন মূল্যমানের নোট গণনা করতে পারে এবং জাল নোট শনাক্ত করতে পারে। উপরন্তু এই এটিএমগুলো এক গ্রাহকের কাছ থেকে প্রাপ্ত একই টাকা অন্য গ্রাহকদের কাছে সরবরাহ করতে পারে। এই ধরনের এটিএম মেশিনকে ক্যাশ-ইন ক্যাশ-আউট এটিএম বা ক্যাশ রিসাইক্লিং মেশিন (CRM) বলা হয়।

একজন গ্রাহকের দ্বারা এটিএম পরিষেবাগুলো পেতে, তার একটি প্লাস্টিক কার্ড ও পিন (ব্যক্তিগত শনাক্তকরণ নম্বর) প্রয়োজন। এই প্লাস্টিক কার্ড ও পিন ব্যাংকে অ্যাকাউন্ট খোলার পরে গ্রাহককে ব্যাংক থেকে সরবরাহ করা হয়।

*একটি পিএসটিএন পিওএস টার্মিনাল*

এই প্লাস্টিকের কার্ডকে এটিএম কার্ড বা ডেবিট কার্ড বলা হয়। গ্রাহক প্রথমে এটিএম-এর একটি স্লটে তার কার্ড প্রবেশ করান এবং এটিএম-এর কীবোর্ড ব্যবহার করে তার পিন টাইপ করেন। তারপরে, একটি মেনু প্রদর্শিত হবে, যা ব্যবহার করে গ্রাহক প্রয়োজনীয় কার্যক্রম সম্পাদন করতে পারবেন। এটিএম কার্ড বা ডেবিট কার্ড ছাড়াও, একজন গ্রাহক এটিএম থেকে টাকা তোলার জন্য তার ক্রেডিট/প্রিপেইড কার্ড ও পিন ব্যবহার করতে পারেন।

### ২.১.২. পিওএস টার্মিনাল (POS Terminal)

একটি সাধারণ পিওএস (পয়েন্ট অব সেল) টার্মিনালে একটি কার্ড থেকে মাইক্রোচিপ এবং ম্যাগনেটিক স্ট্রিপ পড়ার জন্য বিল্ট-ইন ডিভাইস রয়েছে, পিন প্যাডসহ একটি কীবোর্ড, একটি প্রিন্টার এবং একটি পিসি বা ইলেকট্রনিক ক্যাশ রেজিস্ট্রার সংযোগের জন্য একটি পোর্ট রয়েছে। এছাড়াও সাধারণত, পিওএস টার্মিনালটি ব্যাংকের ডেটা সেন্টারে NAC (নেটওয়ার্ক অ্যাক্সেস কন্ট্রোলার) ডায়াল করার ক্ষমতাসহ একটি মডেম দিয়ে সজ্জিত থাকে।

আধুনিক পিওএস টার্মিনালে GPRS কার্যকারিতা রয়েছে, তাই মডেমের পরিবর্তে এটি একটি সিম কার্ড ধারণ করে, যা ব্যবহার করে ডেটা সেন্টারের সঙ্গে সংযোগ স্থাপন করে। সুতরাং এই ধরনের পিওএস টার্মিনাল স্থানান্তরযোগ্য। পিওএস টার্মিনালের স্থানান্তর যোগ্যতা বহাল রাখার জন্য এটির সঙ্গে ব্যাটারি প্রদান করা হয়, যাতে লেনদেনের সময় তা ব্যবহার করা যায়। জিপিআরএস পিওএস টার্মিনালগুলোর সুবিধাগুলো নিম্নরূপ—

ক. পিওএস টার্মিনাল ব্যবহারের জন্য ব্যবসায়ীর পিএসটিএন সংযোগের প্রয়োজন নেই।
খ. গ্রাহককে মার্চেন্টের কাছে কার্ডটি হস্তান্তর করতে হয় না, ফলে কার্ডটি ডুপ্লিকেট হওয়ার সম্ভাবনা নেই।
গ. পিওএস টার্মিনালের পিন প্যাড-এ তার পিন প্রদানের জন্য গ্রাহককে ক্যাশ কাউন্টারে আসতে হবে না।
ঘ. এটি ছোট ভাসমান দোকানে ব্যবহার করা যেতে পারে, যা বিভিন্ন জায়গায় যেমন আবাসিক এলাকা, পার্ক, রেল স্টেশন ইত্যাদিতে পণ্য বিক্রি করে।

ব্যাংকগুলো পিওএস টার্মিনালগুলো কেনে এবং একজন মার্চেন্টকে (দোকান/রেস্তোরাঁ) বিনামূল্যে সরবরাহ করে, একটি সম্মত মার্চেন্ট কমিশনের বিনিময়ে। মার্চেন্ট কমিশন হলো, সরবরাহকৃত পিওএস টার্মিনাল ব্যবহার করে নিষ্পত্তিকৃত বিক্রয়কৃত টাকার পরিমাণের ওপর শতাংশে প্রদেয় কমিশনকে বোঝায়, যা মার্চেন্ট ব্যাংককে প্রদান করে। এটি সাধারণত ১.০% থেকে ২.০% পর্যন্ত হয়।

চুক্তি অনুসারে, একজন ব্যবসায়ীর কমিশনের পরিমাণ গ্রাহকের কাছ থেকে নেওয়া উচিত নয়। যদি একজন মার্চেন্ট তা করেন, তাহলে মার্চেন্টের কাছ থেকে পিওএস টার্মিনাল তুলে নেওয়ার অধিকার সংরক্ষণ করে ব্যাংক।

একটি দোকান থেকে পণ্য বাছাই করার পর, একজন গ্রাহক কাউন্টারে আসেন এবং বিলের নিষ্পত্তির জন্য টেলারের কাছে কার্ডটি হস্তান্তর করেন। যদি কার্ডটি একটি মেগ-স্ট্রিপ কার্ড হয়, তাহলে টেলার একটি দীর্ঘ স্লটে কার্ডটি সোয়াইপ করে আর যদি কার্ডটি একটি চিপভিত্তিক কার্ড হয়, তাহলে টেলার এটিকে একটি স্লটে ঢোকান। টেলার বিল করা টাকার পরিমাণ টাইপ করে এবং গ্রাহককে তার পিন টাইপ করতে বলেন এবং গ্রাহক কীবোর্ডে তার পিন টাইপ করেন। তারপর টেলার একটি 'ওকে' বোতাম টিপেন। পিওএস টার্মিনাল স্বয়ংক্রিয়ভাবে একটি সংরক্ষিত নম্বরে ডায়াল করে এবং ব্যাংকের ডেটা সেন্টারের সঙ্গে সংযুক্ত হয়ে যায়। তারপরে এটি গ্রাহকের অ্যাকাউন্ট থেকে ডেবিট করার এবং মার্চেন্টের অ্যাকাউন্টে ক্রেডিট করার জন্য ব্যাংক সার্ভারে টাকার পরিমাণের সঙ্গে কার্ডের তথ্য স্থানান্তর করে। সার্ভার সফলভাবে ডেবিট/ক্রেডিট করতে পারলে, এটি পিওএস টার্মিনালকে জানিয়ে দেয় এবং পিওএস টার্মিনাল তার প্রিন্টারে একটি অনুমোদন স্লিপ প্রিন্ট করে।

### ২.১.৩ ইন্টারনেট ব্যাংকিং (Internet Banking)

ইন্টারনেট ব্যাংকিং হলো একজন গ্রাহক নিজে তার বাড়িতে বা অফিসে বসে ইন্টারনেটের মাধ্যমে ব্যাংকিং কার্যক্রম সম্পাদন করার একটি উপায়। কোনো কোনো দেশে এটিকে অনলাইন ব্যাংকিংও বলা হয়। ইন্টারনেট ব্যাকিং সুবিধা অ্যাক্সেস করতে গ্রাহকের একটি কম্পিউটার বা স্মার্টফোন এবং একটি ইন্টারনেট সংযোগ থাকলেই চলে। ইন্টারনেট ব্যাকিং সিস্টেম অ্যাক্সেস করার জন্য গ্রাহককে তার ব্যাংক থেকে একটি আইডি (পরিচয়) এবং পাসওয়ার্ড নিতে হয়।

গ্রাহক প্রথমে ব্যাংকের ওয়েবসাইটে যান (একটি ব্রাউজারের ঠিকানা বারে ব্যাংকের ওয়েবসাইটের ঠিকানা টাইপ করে) এবং 'ইন্টারনেট ব্যাকিং' লেখা লিঙ্কটিতে ক্লিক করতে হবে। ইন্টারনেট ব্যাকিং পৃষ্ঠা প্রদর্শিত হলে সেখানে গ্রাহককে তার আইডি ও পাসওয়ার্ড টাইপ করতে হবে। এগুলো সঠিক হলে, গ্রাহক একটি মেনু পাবেন, যা ব্যবহার করে তিনি নিম্নলিখিত কাজগুলো সম্পাদন করতে পারেন—

ক. অ্যাকাউন্টের ব্যালেন্স চেক।
খ. একটি নির্দিষ্ট সময়ের জন্য অ্যাকাউন্ট স্টেটমেন্ট দেখা ও মুদ্রণ করা।
গ. ইউটিলিটি বিল পরিশোধ।
ঘ. যেকোনো মোবাইল ফোন রিচার্জ করা।
ঙ. ঋণের কিস্তি পরিশোধ।
চ. শিক্ষা প্রতিষ্ঠানে ফি প্রদান।
ছ. স্টেন্ডিং ইন্সট্রাকশন যোগ/পরিবর্তন করা বা মুছে ফেলা
জ. গ্রাহকের এসবি/এসটিডি/সিডি অ্যাকাউন্ট থেকে অর্থ ডেবিট করে একটি এফডিআর খোলা।
ঝ. মেয়াদপূর্তিতে বা মেয়াদপূর্তির আগে এফডিআর রিডিম করা (অর্থ এস/এসটিডি/সিডি অ্যাকাউন্টে স্থানান্তর করা হবে)।
ঞ. এলসি ওপেন করা এবং অনুমোদনের জন্য ব্যাংকে পাঠানো।
ট. চেক বইয়ের জন্য একটি অনুরোধ পাঠানো।
ঠ. একটি চেকের পাতায় স্টপ পেমেন্ট করা।
ড. ক্লিয়ারিংয়ের জন্য জমা করা চেকের বর্তমান অবস্থা পরীক্ষা করা।
ঢ. ব্যক্তিগত ঋণের জন্য আবেদন করা।
ণ. সুদের হার পরীক্ষা করা।
ত. মুদ্রার বিনিময় হার পরীক্ষা করা।
থ. পাসওয়ার্ড পরিবর্তন করা, ইত্যাদি।

উল্লেখ্য, ইন্টারনেট ব্যাকিং সিস্টেমে গ্রাহক অর্থ নগদ গ্রহণ বা জমা করতে পারবেন না।

### ২.১.৪. এসএমএস ব্যাংকিং (SMS Banking)

এসএমএস ব্যাকিং হলো, গ্রাহক নিজে তার মোবাইল ফোন থেকে একটি এসএমএস পাঠিয়ে কিছু ব্যাকিং কার্যক্রম সম্পাদন করার একটি উপায়। এসএমএস ব্যাকিং সেবা অ্যাক্সেস করতে, গ্রাহকের মোবাইলটি অবশ্যই ব্যাংকে নিবন্ধিত হতে হবে। ব্যাংক গ্রাহককে একটি পিন প্রদান করবে। তারপর গ্রাহক তার নিবন্ধিত মোবাইল থেকে এসএমএস পাঠিয়ে নিম্নলিখিত কার্যক্রম সম্পাদন করতে পারেন—

ক. অ্যাকাউন্ট ব্যালেন্স চেক করা।
খ. তার অ্যাকাউন্টের একটি মিনি স্টেটমেন্ট পাওয়া।
গ. ইউটিলিটি বিল পরিশোধ।
ঘ. পণ্য ও পরিষেবা ক্রয়ের বিপরীতে বিল পরিশোধ।
ঙ. মোবাইল টপ-আপ করা।
চ. তহবিল স্থানান্তর করা।
ছ. পিন ইত্যাদি পরিবর্তন করা।

উপরোক্ত কাজগুলোর যেকোনো একটি করতে, গ্রাহককে ব্যাংক দ্বারা সংজ্ঞায়িত সিনট্যাক্স অনুসারে একটি এসএমএস লিখতে হবে। উদাহরণস্বরূপ, অ্যাকাউন্ট ব্যালেন্স চেক করার জন্য গ্রাহক লিখতে পারেন: 'BAL ১২৩৪', যেখানে ১২৩৪ তার পিন। তারপরে তিনি ব্যাংকের নির্ধারিত শর্টকোডে যেমন ১৪২১৪ নম্বরে এসএমএস পাঠান। এটি প্রথমে মোবাইল অপারেটরের সিস্টেমে যাবে। অপারেটর হেট যে একটি ব্যাংকের শর্ট কোডটি সেই তথ্য তার কথ্যভাণ্ডারে পূর্বেই সংরক্ষণ করে রেখেছে। মোবাইল অপারেটর মোবাইল নম্বরসহ তার এসএমএসটি ব্যাংক সার্ভারে পাঠাবে। কীওয়ার্ডটি 'BAL' হওয়ায়, ব্যাংক সার্ভার জানে যে গ্রাহক তার অ্যাকাউন্টের ব্যালেন্স খুঁজছেন। সিস্টেম সংশ্লিষ্ট অ্যাকাউন্ট নম্বর (মোবাইল নম্বরের বিপরীতে) খুঁজে বের করবে, ডাটাবেস থেকে অ্যাকাউন্টের ব্যালেন্স (যদি পিন সঠিক থাকে) বের করবে এবং গ্রাহকের মোবাইলে অ্যাকাউন্টের ব্যালেন্সসহ একটি এসএমএস পাঠাবে। ফিরতি এসএমএস নিম্নরূপ হতে পারে—
তারিখ: ৩০/৫/২০১০, সময়: ২৩১০, অ্যাকাউন্ট নং: ৯৯৯৯৯৯৯৯, ব্যালেন্স: টাকা ৯৯৯৯.৯৯

অন্যান্য কার্যকলাপের জন্য বাক্য গঠন নিম্নরূপ হতে পারে:
১. মিনি স্টেটমেন্ট: STM<পিন>
২. ইউটিলিটি বিল পেমেন্ট: UB<পিন> <বিলার কোড> <টাকার পরিমাণ>
৩. ক্রয়ের বিপরীতে অর্থপ্রদান: PAY<পিন> <মার্চেন্ট কোড> <টাকার পরিমাণ>
৪. মোবাইল টপ-আপ: TU<পিন> <মোবাইল নম্বর> <টাকার পরিমাণ>
৫. তহবিল স্থানান্তর: FT<পিন> <অ্যাকাউন্ট নম্বরে> <টাকার পরিমাণ>
৬. পিন পরিবর্তন করুন: PIN <পুরোনো পিন> <নতুন পিন>

### ২.১.৫. অ্যালার্ট ব্যাংকিং (Alert Banking)

অ্যালার্ট ব্যাংকিং হলো এমন একটি সিস্টেম যা গ্রাহকের অ্যাকাউন্টে ডেবিট বা ক্রেডিট লেনদেন হলে গ্রাহককে একটি এসএমএস পাঠায়। উদাহরণস্বরূপ, যদি একজন গ্রাহকের ২৭,০০০/- টাকা মাসিক বেতন তার অ্যাকাউন্টে জমা হয়, তাহলে সিস্টেমটি একটি এসএমএস তৈরি করবে এবং এই মেসেজটি গ্রাহকের নিবন্ধিত মোবাইলে পাঠাবে—
'আপনার অ্যাকাউন্টে ২৩/৪/২০১০ তারিখে ২৩১০-সময়ে ২৭০০০/- টাকা জমা হয়েছে।'

অ্যালার্ট ব্যাকিং গ্রাহকদের জন্য উপযোগী। এর মাধ্যমে তারা তাদের অ্যাকাউন্টে যেকোনো লেনদেন সম্পর্কে তাৎক্ষণিকভাবে জানতে পারে এবং ব্যবস্থা নিতে পারে।

একটি অ্যাকাউন্টের সঙ্গে একটি অ্যালার্ট সেট করতে, ব্যাংককে একজন গ্রাহকের নিকট থেকে নিম্নলিখিতগুলো জানতে হয় ব্যাংককে—
ক. গ্রাহকের মোবাইল নম্বর।
খ. গ্রাহকের অ্যাকাউন্ট নম্বর।
গ. ডেবিট পরিমাণ: টাকা উত্তোলনের পরিমাণের চেয়ে বেশি হলে, একটি ডেবিট অ্যালার্ট তৈরি করা হবে। সাধারণত এই শূন্য সেট করা হয়।
ঘ. ক্রেডিট পরিমাণ: টাকা জমার পরিমাণ এর চেয়ে বেশি হয়, একটি ক্রেডিট অ্যালার্ট তৈরি করা হবে। সাধারণত এই শূন্য সেট করা হয়।

### ২.১.৬. আইভিআর (IVR)

আইভিআর (ইন্টারেক্টিভ ভয়েস রেসপন্স) হলো একটি স্বয়ংক্রিয় ব্যবস্থা যেখানে একজন গ্রাহক তার ল্যান্ড ফোন বা মোবাইল ফোন থেকে কল করতে পারেন এবং কিছু ব্যাকিং পরিষেবা সম্পাদনের জন্য অঙ্ক টিপে মেশিনের সঙ্গে যোগাযোগ করতে পারেন। এই পরিষেবাগুলোর মধ্যে রয়েছে ব্যালেন্স অনুসন্ধান, ফান্ড ট্রান্সফার এবং ডেবিট, ক্রেডিট বা প্রিপেইড কার্ড সক্রিয়/নিষ্ক্রিয় করার মতে ।কার্যাবলি।

আইভিআর এর মাধ্যমে ব্যাকিং করতে গ্রাহককে ব্যাংক থেকে একটি টি-পিন নিতে হয়। তারপর গ্রাহক একটি শর্ট কোড যেমন ৩২২৫ এ কল করবেন। কলটি ব্যাংকের একটি মেশিনে যুক্ত হয়ে যাবে। মেশিনটি গ্রাহককে স্বাগত জানাবে ও জিজ্ঞাসা করবে 'অ্যাকাউন্ট পরিষেবার জন্য ১ টিপুন, কার্ড পরিষেবাগুলোর জন্য ২ টিপুন।' এখন যদি গ্রাহক তার ফোন ডিভাইসের কীবোর্ডে ১ টিপেন, মেশিনটি জিজ্ঞাসা করবে 'অ্যাকাউন্ট ব্যালেন্সের জন্য ১ টিপুন, তহবিল স্থানান্তরের জন্য ২ টিপুন, চেক বইয়ের অনুরোধের জন্য ৩ টিপুন, বিনিময় হারের জন্য ৪ টিপুন, ...' গ্রাহক এখন ১ চাপলে, সিস্টেম তার অ্যাকাউন্টের ব্যালেন্স পড়ে শুনাবে।

## ২.২. ইলেকট্রনিক ব্যাংকিংয়ের সুবিধা ও অসুবিধা

ইলেকট্রনিক ব্যাকিং ব্যবস্থা চালু হওয়ার পর, ব্যাংক কর্মকর্তা ও গ্রাহক উভয়েরই ব্যাকিং করার পদ্ধতিতে একটি আমূল পরিবর্তন এসেছে। ব্যাংক কর্মকর্তাদের ম্যানুয়ালি সমস্ত লেনদেন রেকর্ড করার দরকার নেই। গ্রাহকদের শাখায় লম্বা লাইনে দাঁড়াতে হয় না। ইলেকট্রনিক ব্যাংকিং সিস্টেমের সুবিধা ও অসুবিধাগুলো নিচে উল্লেখ করা হলো—

### ২.২.১. সুবিধাদি

১. গ্রাহকদের টাকা তুলতে ব্যাংকের শাখায় যেতে হবে না। তিনি যে শহরেই থাকেন না কেন, সেই শহরের যে কোনো এটিএম-এ যেতে পারেন এবং সহজেই টাকা তুলতে পারেন।

২. ব্যাংকিং সময়ে গ্রাহকদের টাকা উত্তোলনের বাধ্যবাধকতা নেই। তিনি যে কোনো সময় এটিএম থেকে টাকা তুলতে পারেন, যেমন দিনে বা রাতে, এমনকি ছুটির দিনেও।

৩. একজন গ্রাহক যদি ব্যক্তিগত/অফিসিয়াল/ব্যবসায়িক সফরে যান, তাহলে তাকে তার সঙ্গে বিপুল পরিমাণ অর্থ বহন করতে হবে না। এভাবে টাকা ছিনতাই/চুরির ঝুঁকি এড়ানো যায়।

৪. গ্রাহকদের ইউটিলিটি বিল পরিশোধের জন্য শাখায় যেতে হয় না এবং দীর্ঘ লাইনের মুখোমুখি হতে হয় না। গ্রাহকরা তাদের ইউটিলিটি বিল যেমন বিদ্যুৎ বিল, টেলিফোন বিল, গ্যাস বিল এবং শিক্ষাপ্রতিষ্ঠানের টিউশন ফি যেকোন সময় যেকোন জায়গায় এটিএম ব্যবহার করে, গাড়ি/বাড়ি/অফিসে অবস্থানের সময় বা বিদেশ ভ্রমণের সময় ইন্টারনেট ব্যাংকিং সিস্টেম বা মোবাইল অ্যাপস্ ব্যবহার করে এবং এসএমএস ও আইভিআর সিস্টেম ব্যবহার করে পরিশোধ করতে পারেন, দিনে ২৪ ঘণ্টা, বছরে ৩৬৫ দিন।

৫. গ্রাহককে তার অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে অর্থ স্থানান্তর করতে কোন শাখায় যেতে হয় না। তিনি এটিএম, ইন্টারনেট ব্যাকিং সিস্টেম, মোবাইল অ্যাপস্, এসএমএস সিস্টেম, বা আইভিআর সিস্টেম ব্যবহার করে যেকোনো সময় যেকোনো জায়গা থেকে তার অ্যাকাউন্ট থেকে অন্য একাউন্টে অর্থ স্থানান্তর করতে পারেন।

৬. ইন্টারনেট ব্যাকিং সিস্টেম ব্যবহার করে, গ্রাহক তার এসবি/এসটিডি/সিডি অ্যাকাউন্ট ডেবিট করে একটি এফডিআর খুলতে পারেন। নির্দেশ অনুযায়ী এফডিআর রিডিম করা হবে বা মেয়াদপূর্তিতে পুনঃবিনিয়োগ করা হবে। যদি প্রয়োজন হয়, এফডিআর মেয়াদ পূর্ণ হওয়ার পূর্বেও ভাঙানো যেতে পারে।

৭. গ্রাহককে বিপুল পরিমাণ অর্থ নিয়ে বাজারে যাওয়ার দরকার নেই। তিনি তার বিল পরিশোধ করতে পস টার্মিনালে তার কার্ড ব্যবহার করতে পারেন। এটি তহবিল বহন করার ঝুঁকি হ্রাস করে। অন্যদিকে, দোকানের মালিকদেরও তাদের কাউন্টারে প্রচুর নগদ রাখা থেকে অব্যাহতি দেয়, ফলে দোকান থেকে ব্যাংকে অর্থ স্থানান্তরের সময় রাস্তায় চুরি বা ছিনতাইয়ের ঝুঁকি কমে।

৮. যদি গ্রাহক একজন বেতনধারী হন, তবে তিনি তার অ্যাকাউন্টে তার বেতন জমা দেওয়ার সময় একটি অ্যালার্ট বার্তা পান। এভাবে তিনি সর্বদা তার অ্যাকাউন্টের স্ট্যাটাস সম্পর্কে আপডেট থাকেন।

৯. কোনো গ্রাহকের অ্যাকাউন্টে বিদেশি রেমিট্যান্স জমা হলে, তিনি তার মোবাইল ফোনে একটি তাৎক্ষণিক এসএমএস পান যা তাকে রেমিট্যান্সের পরিমাণ সম্পর্কে অবহিত করে। সুতরাং বিদেশ থেকে তার নিকটাত্মীয়দের পাঠানো রেমিট্যান্সের অবস্থা নিয়ে গ্রাহককে চিন্তামুক্ত রাখে।

১০. তার অ্যাকাউন্টে কোনো অস্বাভাবিক লেনদেন ঘটলে, তিনি তাৎক্ষণিকভাবে তা জানতে পারেন এবং সময়মতো ব্যাংকে অভিযোগ করতে পারেন। ভবিষ্যতে তার অ্যাকাউন্ট/কার্ডে এই ধরনের প্রতারণামূলক কার্যকলাপ এড়াতে প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য তিনি ব্যাংককে অবহিত করতে পারেন।

১১. ইলেকট্রনিক ব্যাকিং ব্যবস্থা প্রবর্তনের পর, অধিকাংশ গ্রাহক নিজেরাই ব্যাংকিং কার্যক্রম সম্পাদন করেন। ফলে, ব্যাংক কর্মকর্তারা তাদের সময় অন্য কাজে ব্যয় করার সুযোগ পান। কম কর্মী ব্যবহার করে ব্যাংকগুলো গ্রাহকদের আরও বেশি পরিষেবা দিতে পারে।

১২. গ্রাহক তার জমাকৃত অর্থের ওপর বেশি নিয়ন্ত্রণ রাখতে পারে।

১৩. ইলেকট্রনিক ব্যাংকিং পরিষেবাগুলোর জন্য, প্রতি-লেনদেনের খরচ সর্বনিম্ন। তাই ব্যাংক এই ধরনের পরিষেবার জন্য গ্রাহকদের কাছ থেকে অল্প পরিমাণ ফি চার্জ করতে পারে।

১৪. যেহেতু গ্রাহকের অর্থের ওপর আরও ভালো নিয়ন্ত্রণ থাকে এবং অর্থ যে কোনো জায়গায় যেকোনো সময় সহজলভ্য, তাই গ্রাহকরা ইলেকট্রনিক ব্যাকিং পরিষেবা প্রদানকারী ব্যাংকে তাদের সমস্ত আমানত রাখেন। এর ফলে ব্যাংকের স্বল্পমূল্যের আমানত বৃদ্ধি পায় এবং ফলস্বরূপ ব্যাংকের মুনাফাও বৃদ্ধি পায়।

### ২.২.২. অসুবিধা

১. গ্রাহকরা এটিএম থেকে এক দিনে নির্দিষ্ট পরিমাণের বেশি এবং নির্ধারিত বারের চেয়ে বেশি টাকা তুলতে পারবেন না। উদাহরণস্বরূপ, একটি নির্দিষ্ট ব্যাংক প্রতি উত্তোলনের পরিমাণ ২০,০০০/- টাকা নির্ধারণ করতে পারে, প্রতিদিন মোট উত্তোলনের পরিমাণ ৫০,০০০/- টাকা এবং গ্রাহকরা প্রতিদিন ৫ বার টাকা উত্তোলন করতে পারবেন। এরূপ ক্ষেত্রে, যদি গ্রাহককে দৈনিক

৫০,০০০/- টাকার বেশি উঠাতে হয়, তবে তাহাকে ব্যাংকের শাখায় যেতে হবে।

২. এটিএম হার্ডওয়্যার বা সফ্টওয়্যারের ত্রুটির কারণে বা এটিএম ভল্টে টাকা ফুরিয়ে যাওয়ার কারণে গ্রাহকরা এটিএম থেকে টাকা নাও পেতে পারেন।

৩. ইন্টারনেট ব্যাংকিং, মোবাইল অ্যাপস্, পিওএস টার্মিনাল, এসএমএস বা আইভিআর সিস্টেমের মাধ্যমে নগদ টাকা তোলা বা জমা করা যায় না।

৪. ইন্টারনেট ব্যাকিং সিস্টেম অ্যাক্সেস করার জন্য গ্রাহকদের অবশ্যই একটি ইন্টারনেট সংযোগসহ একটি কম্পিউটার থাকতে হবে।

৫. যদি একজন হ্যাকার একজন গ্রাহকের ইন্টারনেট ব্যাকিং সিস্টেমের পাসওয়ার্ড জানতে পারে, তাহলে সে অন্য একটি অ্যাকাউন্টে টাকা স্থানান্তর করতে পারে এবং তারপর এটিএম থেকে তা তুলে নিতে পারে।

৬. এটিএম/পিওএস থেকে ব্যাংকের ডেটা সেন্টারে তথ্য স্থানান্তরের সময় যদি কোনো হ্যাকার কোনো গ্রাহকের পিন এবং কার্ডের তথ্য ক্যাপচার করতে পারে তবে ঐ সমস্ত তথ্য দিয়ে সে একটি ডুপ্লিকেট কার্ড তৈরি করে নিতে পারে এবং এটিএম থেকে গ্রাহকের সমস্ত হাতিয়ে নিতে করতে পারে। হ্যাকাররা এটিএম-এ একটি স্কিমিং ডিভাইস ইনস্টল করে কার্ডের তথ্য ও পিন সংগ্রহ করে থাকে।

৭. এসএমএস যোগাযোগের নিরাপদ মাধ্যম নয়। তাই এসএমএস ব্যবহার করে ব্যাংকিং কার্যক্রমও নিরাপদ নয়।

৮. ইলেকট্রনিক ব্যাংকিং ব্যবস্থা প্রযুক্তি-চালিত। তাই গ্রাহকদের কিছু মৌলিক প্রযুক্তি-চালিত অপারেশন জানতে হয়।

৯. ইলেকট্রনিক ব্যাংকিং সিস্টেমের ইনস্টলেশন ও রক্ষণাবেক্ষণের জন্য ব্যাংকের দক্ষ জনবলের একটি বড় দল প্রয়োজন।

১০. ইলেকট্রনিক ব্যাংকিং সিস্টেমের সেটআপ ও চলমান রক্ষণাবেক্ষণ অত্যন্ত ব্যয়বহুল।

১১. ইলেকট্রনিক ব্যাংকিং সিস্টেমে সাইবার হামলার আশংকা অনেক বেশি এবং তার মোকাবেলাও অনেক ব্যয়বহুল।

## ২.৩. অনলাইন ব্যাংকিং

কিছু দেশে, অনলাইন ব্যাংকিং বলতে ইন্টারনেট ব্যাংকিং সিস্টেমকে বোঝায়। যাহোক, আমাদের দেশে, অনলাইন ব্যাংকিং মানে একটি কেন্দ্রীভূত কোর ব্যাংকিং সিস্টেম ইনস্টল করা বোঝায় যেখানে সমস্ত শাখা একটি ওয়্যান (ওয়াইড এরিয়া নেটওয়ার্ক) ব্যবহার করে সংযুক্ত থাকে এবং গ্রাহকরা ব্যাংকের যে কোনো শাখায় ব্যাংকিং করতে পারেন। এটিকে 'অ্যানি ব্রাঞ্চ ব্যাংকিং' হিসাবেও অভিহিত করা হয়। অনলাইন ব্যাংকিং বা অ্যানি ব্রাঞ্চ ব্যাংকিংয়ের সুবিধা ও অসুবিধাগুলো নিম্নরূপ—

### ২.৩.১. সুবিধাদি

১. যদি একটি ব্যাংকে অনলাইন ব্যাংকিং ব্যবস্থা চালু হয়, তাহলে একটি শাখার গ্রাহক সমগ্র ব্যাংকের গ্রাহক হয়ে যায়। এভাবে তিনি যেকোনো শাখা থেকে টাকা তুলতে পারেন বা ব্যাংকের যেকোনো শাখায় টাকা জমা দিতে পারবেন। এছাড়াও তিনি তার পছন্দের যেকোনো শাখা থেকে সমস্ত লেনদেন করতে পারেন। যেমন— গ্রামব্যালেন্স অনুসন্ধান, অ্যাকাউন্ট স্টেটমেন্ট সংগ্রহ, চেক বইয়ের জন্য অনুরোধ করা, পেমেন্ট অর্ডার (পিও) বা ডিমান্ড ড্রাফ্ট (ডিডি) সংগ্রহ করা, এলসি খোলা, বৈদেশিক মুদ্রা ক্রয়/বিক্রয়, বৈদেশিক রেমিট্যান্স গ্রহণ ইত্যাদি।

২. যদি একজন গ্রাহক ব্যক্তিগত/অফিসিয়াল/ব্যবসায়িক উদ্দেশ্যে অন্য শহরে যান, তবে তাকে তার সঙ্গে টাকা বহন করতে হবে না। তিনি ওই শহরের একটি শাখা থেকে টাকা তুলতে পারেন।

৩. যদি একজন গ্রাহক অন্য শহরে ভ্রমণ করার সময় তার ব্যবসায়িক অংশীদারের কাছ থেকে অর্থ গ্রহণ করেন, তবে তাকে তার সঙ্গে সমস্ত অর্থ বহন করে আনার প্রয়োজন নেই। তিনি ওই শহরের যেকোনো ব্যাংকের শাখায় টাকা জমা রাখতে পারেন।

৪. পে-অর্ডার বা ডিডি পাঠানোর দরকার পড়ে না। গ্রাহক সরাসরি তার ব্যবসায়িক অংশীদারদের অ্যাকাউন্টে টাকা জমা দিতে পারেন।

৫. অনলাইন ব্যাকিং ব্যবস্থায়, সমস্ত গ্রাহকের তথ্য এবং লেনদেন কেন্দ্রীয়ভাবে একটি ডেটা সেন্টারে সংরক্ষণ করা হয়। সুতরাং প্রতিটি শাখায় বিশাল আইটি অবকাঠামো স্থাপন ও রক্ষণাবেক্ষণের এবং আইটি বিশেষজ্ঞদের প্রয়োজন নেই।

৬. ব্যাংকগুলোতে কোর ব্যাকিং সিস্টেম স্থাপনের কারণে, এটিএম নেটওয়ার্ক, পিওএস নেটওয়ার্ক, ইন্টারনেট ব্যাকিং সিস্টেম, এসএমএস ব্যাকিং সিস্টেম, অ্যালার্ট ব্যাকিং সিস্টেম, আইভিআর সিস্টেম ইত্যাদির মতো বিভিন্ন ডেলিভারি চ্যানেল চালু করা সম্ভব হয়েছে।

### ২.৩.২. অসুবিধা

১. একটি অনলাইন ব্যাকিং ব্যবস্থা চালু করার জন্য, সমস্ত শাখাকে একটি ওয়্যান (ওয়াইড এরিয়া নেটওয়ার্ক) এর আওতায় আনতে হয়। ওয়্যান-এর জন্য প্রয়োজনীয় যোগাযোগ অবকাঠামো দেশের সব এলাকায় পাওয়া যায় না।

২. অনলাইন ব্যাংকিং ব্যবস্থা চালু হওয়ার পর সমস্ত ব্যাংকিং কার্যক্রম কম্পিউটারের ওপর নির্ভরশীল হয়ে পড়ে। তাই দীর্ঘক্ষণ বিদ্যুৎ না থাকলে ওই সময়ের জন্য সব ব্যাংকিং কার্যক্রম বন্ধ হয়ে যায়। গ্রামীণ এলাকায় যেখানে সার্বক্ষণিক বিদ্যুৎ সরবরাহ বিরল সেখানে অনলাইন ব্যাংকিং ব্যবস্থার জন্য এটি একটি চ্যালেঞ্জ হয়ে দাঁড়ায়।

৩. অনলাইন ব্যাংকিং সিস্টেম পরিচালনার জন্য, একটি শাখার সমস্ত কর্মচারীকে কম্পিউটার নলেজে প্রশিক্ষিত হতে হয়।

৪. কখনও কখনও, যোগাযোগ নেটওয়ার্ক বন্ধ হয়ে যায় (ব্রেক ডাউন)। এই ধরনের ক্ষেত্রে, শাখাটি ডেটা সেন্টার থেকে সংযোগ বিচ্ছিন্ন হয়ে যায় এবং এ সময় কোনও লেনদেন করা যায় না। এতে গ্রাহকদের ভোগান্তির সৃষ্টি হয়।

৫. একটি কেন্দ্রীয় ডেটা সেন্টার তৈরি করা, কোর ব্যাংকিং সফ্টওয়্যার ইনস্টল করা, ওয়্যান সেটআপ করা এবং প্রতিটি কর্মচারীর জন্য সমস্ত শাখায় কম্পিউটার সরবরাহ করা অত্যন্ত ব্যয়বহুল।

৬. অনলাইন ব্যাংকিং সেটআপ এবং রক্ষণাবেক্ষণ অত্যন্ত জটিল কার্যকলাপ। এর জন্য খুব উচ্চতর বিশেষজ্ঞ আইটি টিম প্রয়োজন। এমন একটি দল সহজে মেলে না। তাছাড়াও অনেক ব্যয়বহুল।

৭. কেন্দ্রীভূত সফ্টওয়্যারের দাম বিকেন্দ্রীভূত সফ্টওয়্যারের দামের তুলনায় অনেক বেশি।

৮. অনলাইন ব্যাংকিং ব্যবস্থায় সাইবার হামলার আশংকা বেশি।

## ৩. মোবাইল আর্থিক পরিষেবা

মোবাইল ফাইন্যান্সিয়াল সার্ভিসেস (MFS) হল প্রধানত ব্যাংকবহির্ভূত জনগোষ্ঠীর জন্য একটি ব্যাকিং ব্যবস্থা যা ব্যবহার করে একজন নিবন্ধিত মোবাইল ব্যবহারকারী এজেন্টের কাছ থেকে টাকা জমা (ক্যাশ-ইন) এবং উত্তোলন (ক্যাশ-আউট) করতে পারেন, তার এমএফএস অ্যাকাউন্ট থেকে অন্য এমএফএস অ্যাকাউন্টে অর্থ স্থানান্তর করতে পারেন (পি২পি) এবং বিদেশ থেকে রেমিট্যান্স গ্রহণ করা, কেনাকাটার বিল (মার্চেন্ট পে) এবং ইউটিলিটি বিল (বিল পে) পরিশোধ করা, বেতন এবং বিভিন্ন সরকারি ভাতা ও উপবৃত্তি গ্রহণ করা এবং তার নিজের/আত্মীয়দের মোবাইলের জন্য এয়ারটাইম ক্রয় করা ইত্যাদি কার্যক্রম সম্পন্ন করতে পারেন।

দোকানে বিল পেমেন্ট করা হলো একটি পি২বি (ব্যবসায়িক ব্যক্তি) কার্যকলাপ যাকে মার্চেন্ট পেমেন্টও বলা হয়। এমএফএস-এর এই ফাংশনটি ব্যবহার করে, গ্রাহক একটি দোকান বা রেস্তোরাঁ থেকে (যাকে মার্চেন্ট বলা হয়) পণ্য ও পরিষেবা কিনতে পারেন এবং তার মোবাইল অ্যাকাউন্ট থেকে মার্চেন্টের মোবাইল অ্যাকাউন্টে অর্থ স্থানান্তর করে বিল পরিশোধ করতে পারেন।

২০১১ সালে বাংলাদেশে এমএফএস এর শুরুতে, দেশের জনসংখ্যার মাত্র ১৩%-এর একটি ব্যাংক অ্যাকাউন্ট ছিল যেখানে ৪৫% জনগণ একটি মোবাইল ফোনের ব্যবহারকারী ছিল। সুতরাং মনে করা হয়েছিল যে মোবাইল ব্যাংকিং প্রযুক্তি ব্যবহার করে, একটি বিশাল জনসংখ্যাকে ব্যাংকিং ব্যবস্থায় আনা যাবে। গ্রামীণ এলাকায় যেখানে কোন ব্যাংকের শাখা নেই, সেখানে ব্যাংকিং কার্যক্রম সম্প্রসারিত করা যাবে। এতে দেশি-বিদেশি অনানুষ্ঠানিক রেমিট্যান্স বা হুন্ডি বন্ধ হয়ে যাবে।

সেই অনুসারে, লাইসেন্স প্রদানের জন্য প্রয়োজনীয় গাইডলাইন ও পলিসি তৈরির পূর্বেই বাংলাদেশ ব্যাংক ডাচ্-বাংলা ব্যাংক ও ব্র্যাক ব্যাংককে মোবাইল ফিন্যান্সিয়াল সার্ভিস চালু করার জন্য এনওসি প্রদান করে। ডাচ্-বাংলা ব্যাংক মার্চ, ২০১১ সালে 'রকেট' শিরোনামে তাদের এমএফএস এবং জুন, ২০১১ সালে ব্র্যাক ব্যাংক 'বিকাশ' নামে এমএফএস শুরু শুরু করে। এরপর অন্য ব্যাংকগুলো একে একে তাদের নিজস্ব এমএফএস সেবা চালু করে। নবীনতম অন্যান্য এমএফএসগুলো হলো, বাংলাদেশ পোস্ট অফিসের 'নগদ' ও ট্রাস্ট ব্যাংকের 'ট্যাপ' এবং ইউসিবি ব্যাংকের 'উপায়'।

পরবর্তীকালে বাংলাদেশ ব্যাংক 'এমএফএস' নীতি প্রণয়ন করে যার অধীনে এমএফএস অপারেটরদের লাইসেন্স দেওয়া হয়। বিদ্যমান নীতিমালা অনুযায়ী, বাংলাদেশে এমএফএস মডেলটি ব্যাংক পরিচালিত, যার মানে একটি এমএফএস-এ, একটি ব্যাংকের কমপক্ষে ৫১% শেয়ার বজায় রাখতে হবে।

বাংলাদেশে এমএফএস-এর ১১ বছর যাত্রার পর, এটি কেনিয়ার পরে বিশ্বের ২য় বৃহত্তম এমএফএস বাজার। বাংলাদেশ ব্যাংকের প্রতিবেদন অনুসারে, বর্তমানে (ফেব্রুয়ারি, ২০২২ পর্যন্ত) এমএফএস-এ নিবন্ধিত গ্রাহকের সংখ্যা ৮১.৮৬ মিলিয়ন যার মধ্যে সক্রিয় গ্রাহকের সংখ্যা ২৭.০৮ মিলিয়ন। প্রায় ১০ মিলিয়ন এজেন্ট এই গ্রাহকদের পরিষেবা প্রদান করছে। ২০২২ সালের ফেব্রুয়ারি মাসে (এক মাসের জন্য) মোট লেনদেনের সংখ্যা ২২৬ মিলিয়ন এবং এই সময়ের মধ্যে মোট লেনদেনের পরিমাণ ছিল ৪১৩ বিলিয়ন টাকা। ৪১৩ বিলিয়ন টাকার লেনদেনের মধ্যে নিম্নলিখিতগুলো অন্তর্ভুক্ত ছিল—

১. ক্যাশ-ইন লেনদেন: ১৪৬ বিলিয়ন
২. ক্যাশ-আউট লেনদেন: ১৩৭ বিলিয়ন
৩. পি২পি লেনদেন: ৯৮ বিলিয়ন
৪. বেতন বিতরণ: ১১ বিলিয়ন
৫. মার্চেন্ট পেমেন্ট: ৫.৮ বিলিয়ন

৬. ইউটিলিটি বিল পেমেন্ট: ৪.৪ বিলিয়ন
৭. সরকারি অর্থপ্রদান: ২.৮ বিলিয়ন
৮. অভ্যন্তরীণ বৈদেশিক রেমিট্যান্স: ০.৩ বিলিয়ন
৯. অন্যান্য (রিচার্জসহ): ৭.৭ বিলিয়ন

## ৪. এজেন্ট ব্যাংকিং

অল্প শিক্ষিত বা অশিক্ষিত গ্রামীণ ক্লায়েন্টদের জন্য কোর ব্যাংকিং কার্যক্রম পরিচালনা করা জটিল, কারণ তারা তাদের নিজ নিজ ব্যাংক অ্যাকাউন্ট থেকে অর্থ উত্তোলনের জন্য প্রয়োজনীয় একটি চেক লিখতে এবং স্বাক্ষর করতে পারে না। তারা এটিএম থেকে টাকা তোলার জন্য তাদের ডেবিট কার্ডের পিন মনে রাখতে ও ইনপুট করতে পারে না।

অন্যদিকে, তাদের নিজ নিজ মোবাইল ব্যাংকিং অ্যাকাউন্ট (এমএফসি অ্যাকাউন্ট) থেকে টাকা তোলার ক্ষেত্রে তাদের নিজ নিজ মোবাইল ফোন ব্যবহার করে পিন প্রদান করতে হয়, যা তারা মনে রাখতে পারে না এবং মোবাইল ফোনে টাইপ করতে পারে। তাই মোবাইল ব্যাংকিং গ্রামীণ অশিক্ষিত গ্রাহকদের জন্য উপযুক্ত নয়।

এই সমস্যাগুলো কাটিয়ে উঠতে, ২০১৫ সালে বাংলাদেশের সেন্ট্রাল ব্যাংক কর্তৃক এজেন্ট ব্যাংকিংয়ের ধারণাটি শুরু করা হয়েছিল যেখানে একটি ডিভাইসে আঙুলের ছাপ চেপে সমস্ত লেনদেন অনুমোদিত হবে। এজেন্ট ব্যাংকিং-এ বৈদেশিক মুদ্রার লেনদেন ছাড়া সব ধরনের ব্যাংকিং লেনদেন অনুমোদিত। এজেন্ট আউটলেটগুলো গ্রামীণ এলাকায় সংশ্লিষ্ট ব্যাংকগুলোর দ্বারা লাইসেন্সপ্রাপ্ত যা ব্যাংকের পক্ষে লেনদেনগুলো সম্পাদন করে। এজেন্টরা তাদের ডিপোজিটের পরিমান, অ্যাকাউন্ট খোলা এবং বৈদেশিক রেমিট্যান্স বিতরণ ও লোন প্রদানের জন্য কমিশন পান। এজেন্ট আউটলেটগুলো শুধু একটি নির্দিষ্ট ব্যাংকের লেনদেন করতে পারে এবং তাদের আউটলেটে অন্য কোন ধরনের ব্যবসা করার অনুমতি নেই।

বাংলাদেশে এজেন্ট ব্যাংকিংয়ের বর্তমান অবস্থা নিচে দেওয়া হলো (৩১ জুন, ২০২২ অনুযায়ী)—

লাইসেন্সসহ ব্যাংকের সংখ্যা: ৩০
এজেন্ট আউটলেট সংখ্যা: ১৯,৭৩৭
এজেন্ট ব্যাংকিং অ্যাকাউন্টের সংখ্যা: ১৬,০৭৪,৩৭৮
মহিলা অ্যাকাউন্টের সংখ্যা: ৭,৯৩৭,৮৬৭
গ্রামীণ অ্যাকাউন্টের সংখ্যা: ১৩,৮৯০,৩২১
জমার পরিমাণ (মিলিয়ন টাকায়): ২৮০,৮৫৩
বিতরণ করা ঋণের পরিমাণ (মিলিয়ন টাকায়): ৭৬,৪৫৬
ইনওয়ার্ড রেমিট্যান্সের পরিমাণ (মিলিয়ন টাকায়): ৯৭০,৪৮১

(সূত্র : বাংলাদেশ ব্যাংক)

## ৫. ই-কমার্স এবং এম-কমার্স

### ৫.১. ই-কমার্স

জেমস এ. ও'ব্রায়েনের মতে 'ই-কমার্স হল বিভিন্ন কম্পিউটার নেটওয়ার্কের মাধ্যমে পণ্য, পরিষেবা এবং তথ্যের ক্রয়-বিক্রয় ও বিপণন পদ্ধতি প্রদান করা।' সংক্ষেপে, ইন্টারনেটের মাধ্যমে পণ্য ও পরিষেবার ক্রয়-বিক্রয়কে ই-কমার্স বলা হয়।

এই সিস্টেমে, বিক্রেতা (মার্চেন্ট) একটি ওয়েবসাইট তৈরি করে যেখানে তিনি যে সমস্ত আইটেম বিক্রি করতে চান তা প্রদর্শন করেন। প্রতিটি আইটেমের এক বা একাধিক ছবি, বর্ণনা, স্পেসিফিকেশন ও এলাকাভিত্তিক ডেলিভারি সময় উল্লেখ থাকবে। গ্রাহক ওয়েবসাইট পরিদর্শন করেন এবং তিনি যে আইটেমগুলো কিনতে চান তা নির্বাচন করেন। বাছাইকৃত আইটেমগুলোকে এমন জায়গায় রাখা হয়েছে যাকে কার্ট (CART) বলা হয়। নির্বাচন শেষ হলে, ক্রেতা ডেলিভারির ঠিকানা টাইপ করেন (যদি আগে নিবন্ধিত না হয়ে থাকে) এবং বিল পরিশোধ করতে 'চেক-আউট' বোতাম চাপেন।

মার্চেন্টের ওয়েবসাইটটি একটি ব্যাংকের ই-কমার্স সিস্টেমের সঙ্গে যুক্ত। ব্যাংকের ই-কমার্স সিস্টেম 'পেমেন্ট গেটওয়ে' বা 'পেমেন্ট সুইচ' নামে পরিচিত। যে ব্যাংকের সঙ্গে মার্চেন্ট সংযুক্ত থাকে তা এ্যাকুয়ারিং ব্যাংক বা এ্যাকুয়ারার হিসাবে পরিচিত। ক্রেতা চেক-আউট বোতামে ক্লিক করার পরে, ক্রেতার মনিটরে একটি নতুন উইন্ডো প্রদর্শিত হবে যেখানে তিনি তার ডেবিট কার্ড বা ক্রেডিট কার্ড নম্বর, পিন/সিভিভি/সিভিসি, মেয়াদ শেষ হওয়ার তারিখ ইত্যাদি টাইপ করবেন এবং 'কনফার্ম' বাটনে ক্লিক করবেন। পিন মানে ব্যক্তিগত শনাক্তকরণ নম্বর, সিভিভি মানে কার্ড ভেরিফিকেশন ভ্যালু (ভিসা দ্বারা ব্যবহৃত) এবং সিভিসি মানে কার্ড ভেরিফিকেশন কোড (মাস্টারকার্ড ব্যবহার করে।)

পেমেন্ট গেটওয়ে কার্ডের তথ্য সংগ্রহ করে এবং সঠিকতার জন্য তথ্য পরীক্ষা করে। সরবরাহকৃত তথ্য সঠিক পাওয়া গেলে, সিস্টেম উল্লিখিত টাকা ক্রেতাদের ব্যাংক অ্যাকাউন্ট বা ক্রেডিট কার্ড অ্যাকাউন্ট থেকে ডেবিট করে এবং মার্চেন্টের অ্যাকাউন্টে ক্রেডিট করে। তারপর সিস্টেম উভয় পক্ষকে কর্ম সম্পর্কে অবহিত করে।

যদি কার্ডটি একই ব্যাংকের না হয়, তাহলে পেমেন্ট গেটওয়ে প্রযোজ্য পেমেন্ট অ্যাসোসিয়েশনের কাছে তথ্য পাঠায় (NPSB, মাস্টারকার্ড, ভিসা, অ্যামেক্স,

জেবিসি, দিনার, ডিসকভার ইত্যাদির নেটওয়ার্ক)। পেমেন্ট অ্যাসোসিয়েশন তারপর কার্ডের তথ্য ইস্যুকারী ব্যাংককে পাঠায়। ইস্যুকারী ব্যাংক হলো এমন একটি ব্যাংক, যা গ্রাহককে কার্ড ইস্যু করে থাকে।

এখন ইস্যুকারী ব্যাংক কার্ডের তথ্য যাচাই করে এবং সঠিক পাওয়া গেলে ক্রেতার ব্যাংক অ্যাকাউন্ট বা কার্ড অ্যাকাউন্ট ডেবিট করে। একে লেনদেনের অথোরাইজেশন বলে। অনুমোদনের বার্তাটি এ্যাকোয়ারিং ব্যাংকে যায়, যা ঐ পরিমান টাকা মার্চেন্টের অ্যাকাউন্টে (সাধারণত অফলাইন) ক্রেডিট করে এবং উভয় পক্ষকে পদক্ষেপ সম্পর্কে অবহিত করে।

যে উপায়ে এ্যাকোয়ারিং ব্যাংক ইস্যুকারী ব্যাংকের কাছ থেকে অর্থ পায়, যদি এগুলো ভিন্ন হয়, তাকে স্যাটেলম্যান্ট বলে। পেমেন্ট অ্যাসোসিয়েশনগুলো প্রতিদিনই ইস্যুকারী ব্যাংকের নস্ট্রো অ্যাকাউন্ট ডেবিট করে এবং অধিগ্রহণকারী ব্যাংকের নস্ট্রো অ্যাকাউন্টে ক্রেডিট করে স্যাটেলম্যান্ট কার্যক্রম সম্পন্ন করে থাকে। এনপিএসবি (ন্যাশনাল পেমেন্ট সুইচ, বাংলাদেশ) এর মাধ্যমে রুট করা অভ্যন্তরীণ লেনদেনের ক্ষেত্রে, নস্ট্রো অ্যাকাউন্ট হলো বাংলাদেশ ব্যাংকের (কেন্দ্রীয় ব্যাংক) সঙ্গে রক্ষিত সংশ্লিষ্ট ব্যাংকগুলোর অ্যাকাউন্ট, কিন্তু পেমেন্ট অ্যাসোসিয়েশনগুলোর নেটওয়ার্ক ব্যবহার করে করা লেনদেনের ক্ষেত্রে, নস্ট্রো অ্যাকাউন্ট হলো একটি বিদেশি ব্যাংকের সঙ্গে স্থানীয় ব্যাংক কর্তৃক খোলা একটি অ্যাকাউন্ট।

এ্যাকোয়ারিং ব্যাংক থেকে প্রাপ্ত তথ্যের ওপর নির্ভর করে, মার্চেন্ট ক্রেতাদের ঠিকানায় পণ্য এবং পরিষেবা সরবরাহ করে।

পেমেন্ট গেটওয়ে ব্যবহার করে, কার্ডধারীরা ইউটিলিটি বিল যেমন বিদ্যুৎ, গ্যাস, পানি, টেলিফোন বিল, টিউশন ফি, আয়কর, সিটি কর্পোরেশন ট্যাক্স, এবং ট্রেন, বিমান, বাস, স্টিমার, সিনেমা, নাটক ইত্যাদির টিকিট কিনতে পারে। তবে এই ধরনের সমস্ত কোম্পানির একটি ওয়েবসাইট থাকতে হয় যাতে প্রবেশ করে গ্রাহকের রেফারেন্স নম্বর (যেমন মিটার নম্বর, অ্যাকাউন্ট নম্বর, টেলিফোন নম্বর ইত্যাদি) দেওয়ার পর গ্রাহকদের অপরিশোধিত বিল/ফি/ট্যাক্স প্রদর্শন করতে সক্ষম হয়। গ্রাহককে 'পে' বোতামে ক্লিক করে অপরিশোধিত বিল পরিশোধ করতে সক্ষম হন। টিকিট কেনার ক্ষেত্রে, গ্রাহকদের খালি আসনগুলো দেখতে এবং একটি লেআউট থেকে তাদের পছন্দসই আসন নির্বাচন করার সুযোগ দিতে হবে।

### ৫. ২. এম-কমার্স

এম-কমার্স (বা মোবাইল কমার্স) হলো ওয়্যারলেস হ্যান্ডহেল্ড ডিভাইস যেমন সেলুলার টেলিফোন এবং ব্যক্তিগত ডিজিটাল সহকারী (PDAs) এর মাধ্যমে পণ্য ও পরিষেবার ক্রয় ও বিক্রয়। এম-কমার্স হল মোবাইল ব্যাকিং সিস্টেম দ্বারা অফার করা অনেকগুলো ক্রিয়াকলাপের মধ্যে একটি। এম-কমার্স একটি উদীয়মান প্রযুক্তি, যা ওয়্যারলেস অ্যাপ্লিকেশন প্রোটোকল (WAP) এর ওপর ভিত্তি করে তৈরি। এটি প্রায় সমস্ত দেশে অনেক বেশি অগ্রগতি করেছে। আজকাল ই-কমার্স এবং এম-কমার্সের মধ্যে কোনো পার্থক্য নেই কারণ সমস্ত ক্রেতা কম্পিউটার ও মোবাইল ব্যবহার করে সমানভাবে সমস্ত পণ্য এবং পরিষেবা কিনতে পারেন।

## ৬. কম্পিউটার হার্ডওয়্যার

একটি কম্পিউটার হল একটি ইলেকট্রনিক ডিভাইস, যা মানুষের জন্য ফলাফল নির্ণয় ও প্রদর্শন করার উদ্দেশ্যে মানুষের দেওয়া যুক্তি ও সূত্র ব্যবহার করে মানুষের দ্বারা সরবরাহ করা ডেটা এবং তথ্য দ্রুত এবং সঠিকভাবে প্রক্রিয়া করে। মানুষ এই ফলাফলের ওপর ভিত্তি করে সিদ্ধান্ত গ্রহণ করে।

### ৬.১. কম্পিউটারের বিকাশের ইতিহাস

একটি কম্পিউটার শত শত বছরের গবেষণার ফলাফল। জন নেপিয়ার (১৫৫০-১৬১৭), ব্লেস প্যাস্কাল (১৬৪২), এবং লাইবনিজ (১৬৭১) এর মতো গণিতবিদদের গণনাযন্ত্রের আবিষ্কারের মাধ্যমে কম্পিউটারের বিকাশ শুরু হয়েছিল। ইংল্যান্ডের গণিতবিদ চার্লস ব্যাবেজ (১৭৯২-১৮৭১), ১৮২১ সালে ডিফারেন্স ইঞ্জিন তৈরি করেন। ১৮৩৩ সালে, তিনি 'অ্যানালিটিকাল ইঞ্জিন' নামে আরেকটি গণনাযন্ত্র তৈরি করতে শুরু করেন, কিন্তু মৃত্যুর আগে এটি শেষ করতে পারেননি। তার বিশ্লেষণাত্মক ইঞ্জিনের নকশা আধুনিক কম্পিউটারের ভিত্তি। এই কারণেই চার্লস ব্যাবেজকে 'কম্পিউটারের জনক' বলা হয়।

মার্কিন যুক্তরাষ্ট্রের অধ্যাপক ডি. জন অ্যাটানাসফ ১৯৪২ সালে ভ্যাকুয়াম টিউব ব্যবহার করে ABC নামে একটি ইলেকট্রনিক কম্পিউটার তৈরি করেন। পরবর্তীতে ১৯৪৬ সালে, অধ্যাপক ড. জন মাউচলি এবং তার ছাত্র ইঞ্জিনিয়ার প্রেসপার যৌথভাবে ENIAC (ইলেক্ট্রনিক নিউমেরিক ইন্টিগ্রেটর অ্যান্ড ক্যালকুলেটর) নামে একটি কম্পিউটার তৈরি করেন যার মধ্যে ১৮০০ ভালভ ছিল। এর ওজন ছিল ৩০ টন, এবং এটি চালানোর জন্য ১৫০ কিলোওয়াট বৈদ্যুতিক লোড প্রয়োজন ছিল। এই দুই বিজ্ঞানী ১৯৫১ সালে UNIVAC (Universal Automatic Calculator) নামে আরেকটি কম্পিউটার তৈরি করেন যার ইনপুট, আউটপুট ও মেমোরি ইউনিট ছিল। এটি ছিল বাণিজ্যিকভাবে উৎপাদিত প্রথম ইলেকট্রনিক কম্পিউটার।

১৯৫৪ সালে, মার্কিন যুক্তরাষ্ট্রের আইবিএম (International Business Machine) কোম্পানি আইএমবি-৭০১ নামে একটি কম্পিউটার তৈরি করে এবং ব্যবসা শুরু করে।

বাংলাদেশ পরমাণু শক্তি কমিশন ১৯৬৪ সালে ঢাকায় প্রথম কম্পিউটার ইনস্টল করে। এটি একটি আইবিএম-১৬২০ মেইনফ্রেম কম্পিউটার ছিল। এরপর বাংলাদেশ প্রকৌশল ও প্রযুক্তি বিশ্ববিদ্যালয় (বুয়েট), বাংলাদেশ পরিসংখ্যান ব্যুরো, পাওয়ার ডেভেলপমেন্ট বোর্ড তাদের ব্যবহারের জন্য মেইনফ্রেম কম্পিউটার স্থাপন করে।

১৯৭১ সালে, মার্কিন যুক্তরাষ্ট্রের ইন্টেল কোম্পানি এমএসসি-৪ মাইক্রোপ্রসেসর তৈরি করে এবং মাইক্রোকম্পিউটার চালু করে। এর উন্নয়ন এবং বাণিজ্যিক প্রাপ্যতার কারণে, আমরা শিক্ষা প্রতিষ্ঠান, ব্যবসায়িক প্রতিষ্ঠান, অফিস এবং বাড়িতে মাইক্রোকম্পিউটার ব্যবহার দেখতে পাচ্ছি।

### ৬.২. কম্পিউটারের প্রজন্ম

কম্পিউটারকে নিম্নলিখিত চারটি প্রজন্মে ভাগ করা যায়—

<u>১ম প্রজন্ম (১৯৫১-১৯৫৮)</u>

বৈশিষ্ট্য : ভ্যাকুয়াম টিউব বা ভ্যাকুয়াম ভালভের ব্যবহার, আকারে বড়, প্রোগ্রাম এবং তথ্য সঞ্চয় করার ক্ষমতা, ম্যাগনেটিক ড্রাম, পাঞ্চ কার্ড ও ম্যাগনেটিক টেপের ব্যবহার। উদাহরণ: ইএনআইএসি, মার্ক, আইবিএম-৬৫০।

<u>২য় প্রজন্ম (১৯৫৮-১৯৬৫)</u>

বৈশিষ্ট্য : আইসি (ইন্টিগ্রেটেড সার্কিট) ব্যবহার, ভ্যাকুয়াম টিউবের পরিবর্তে ট্রানজিস্টরের ব্যবহার, আকারে ছোট, ACCII কোড প্রবর্তন, কোবল, ফোরট্রান ও এলগল-এর মতো উচ্চস্তরের ভাষার বিকাশ। উদাহরণ: আইবিএম-১৬২০, সিডিসি-১৬০৪, এনসিআর-৩০০।

<u>৩য় প্রজন্ম (১৯৬৫-১৯৭১)</u>

বৈশিষ্ট্য : একটি ইনপুট ডিভাইস হিসাবে মাউসের পরিচিতি, আকারে ছোট, দাম হ্রাস, আউটপুট ডিভাইস হিসাবে ভিডিও ইউনিট এবং প্রিন্টার প্রবর্তন, সেকেন্ডারি মেমোরির ব্যবহার, বেসিক ভাষার উদ্ভাবন, শব্দ প্রক্রিয়াকরণ ও অন্যান্য অ্যাপ্লিকেশন। উদাহরণ : আইবিএম-৩৭০, পিডিপি-II।

<u>৪র্থ প্রজন্ম (১৯৭১-আজ পর্যন্ত)</u>

বৈশিষ্ট্য : মাইক্রোপ্রসেসরের উদ্ভাবন এবং ব্যবহার, সেমি-কন্ডাক্টর মেমোরি, রম, র‍্যাম, প্রোম, এ্যাপ রম, তথ্য সংরক্ষণের উচ্চ ক্ষমতা, ডস, ম্যাক, উইন্ডোজ এবং ইউনিক্সের মতো অপারেটিং সিস্টেমের বিকাশ, বিভিন্ন অ্যাপ্লিকেশন সফ্টওয়্যার এবং প্রোগ্রামিং ভাষার বিকাশ, সুপার কম্পিউটার, ল্যাপটপ, নোটবুক, ডেস্কটপ ও পার্সোনাল কম্পিউটারের উন্নয়ন। উদাহরণ : পিসি, সার্ভার এবং বিভিন্ন ব্র্যান্ডের ল্যাপটপ যেমন আইবিএম, কমপ্যাক, এইচপি, সান, ডেল, এচার।

### ৬.৩. কম্পিউটারের শ্রেণিবিভাগ

কাজের প্রকৃতির ওপর ভিত্তি করে, কম্পিউটারকে নিম্নলিখিত তিন প্রকারে ভাগ করা যায়—

১. এনালগ কম্পিউটার।
২. ডিজিটাল কম্পিউটার।
৩. হাইব্রিড কম্পিউটার।

অ্যানালগ কম্পিউটার বিশেষ কাজে ব্যবহার করা হয় যেমন চাপ ও তাপমাত্রা পরিমাপ করা, পেট্রোল পাম্পে পেট্রোল সরবরাহ করা এবং মূল্য নির্ধারণ করা এবং গাড়ি বা বিমানের গতি নিয়ন্ত্রণ করা।

ডিজিটাল কম্পিউটার গণিতের নীতির সঙ্গে সামঞ্জস্য রেখে কাজ করে। এটি বাইনারি সিস্টেম ব্যবহার করে কাজ করে, যেমন, ১ এবং ০ ব্যবহার করে। আমরা বাড়িতে এবং অফিসে যে কম্পিউটারগুলো ব্যবহার করি তা সবই ডিজিটাল কম্পিউটার।

হাইব্রিড কম্পিউটার অ্যানালগ প্রক্রিয়া ব্যবহার করে বিভিন্ন সিস্টেম থেকে ডেটা সংগ্রহ করে কিন্তু ডিজিটাল সিস্টেমে ডেটা প্রক্রিয়া করে।

*একটি সুপার কম্পিউটার*

*একটি মেইনফ্রেম*

আকার ও কর্মক্ষমতা অনুযায়ী কম্পিউটার (বা ডিজিটাল কম্পিউটার) চার প্রকারের হয়ে থাকে, যেমন—

১. সুপার কম্পিউটার

২. মেইনফ্রেম কম্পিউটার
৩. মিনি কম্পিউটার
৪. মাইক্রো কম্পিউটার

সুপার কম্পিউটার খুবই শক্তিশালী। গাণিতিক প্রক্রিয়াগুলো সম্পূর্ণ করতে কম সময় লাগে। সুপার কম্পিউটারগুলো বৈজ্ঞানিক গবেষণা, বিপুল পরিমাণ তথ্য প্রক্রিয়াকরণ, ক্ষেপণাস্ত্র নিয়ন্ত্রণ, মহাকাশ গবেষণা এবং পারমাণবিক প্ল্যান্টের নকশায় ব্যবহৃত হয়। ক্রে-১, সুপার এসএক্সএল, এবং সাইবার-২০৫ সুপার কম্পিউটারের উদাহরণ।

মেইনফ্রেম কম্পিউটার আকারে অনেক বড়। এতে অনেক ছোট-ছোট কম্পিউটার কানেক্ট করে একটি মেইনফ্রেম কম্পিউটারে একসঙ্গে অনেক মানুষ কাজ করতে পারে। এটি ব্যাংক, বীমা কোম্পানি ও বিশ্ববিদ্যালয়গুলোর মতো বড় সংস্থাতে ব্যবহৃত হয়। আইবিএম ৪৩০০, ইউনিভ্যাক ১১০০, এবং এনসিআর ৮৩৭০ হলো মেনফ্রেম কম্পিউটারের উদাহরণ।

মিনি কম্পিউটারগুলো মেইনফ্রেম কম্পিউটারের তুলনায় ছোট এবং কম ব্যয়বহুল। অনেক লোক একটি মিনি কম্পিউটারের সঙ্গে সংযুক্ত টার্মিনাল ব্যবহার করে একসঙ্গে কাজ করতে পারে। তুলনামূলকভাবে ছোট ব্যাংক, বীমা কোম্পানি, শিল্প, শিক্ষা প্রতিষ্ঠান এবং গবেষণা সংস্থাগুলো মিনি-কম্পিউটার ব্যবহার করে। আইবিএম এস/৩৪ এবং এনসিআর এস/৯২৯০ হলো মিনি কম্পিউটারের উদাহরণ।

মাইক্রোকম্পিউটার খুবই ছোট, সস্তা এবং বহুল ব্যবহৃত কম্পিউটার। এই ধরনের কম্পিউটারে মাইক্রোপ্রসেসর ব্যবহার করা হয় বলে এদেরকে মাইক্রোকম্পিউটার বলা হয়। একটি মাইক্রোকম্পিউটারে একবারে মাত্র একজন কাজ করতে পারে। এই জন ব্যক্তিগত কম্পিউটার বা পিসি নামেও পরিচিত। মাইক্রোকম্পিউটার ব্যক্তিগত এবং অফিসিয়াল উদ্দেশ্যে বাড়িতে এবং অফিসে ব্যবহার করা হয়। এগুলো গেম খেলা, ভিডিও দেখা, গান শোনা এবং ইন্টারনেট ব্রাউজ করার মতো বিনোদনের উদ্দেশ্যেও ব্যবহৃত হয়। আইবিএম পিসি, অ্যাপল পিসি, এবং ম্যাকিনটোশ পিসি হলো মাইক্রোকম্পিউটারের উদাহরণ।

## ৬.৪. কম্পিউটার হার্ডওয়্যার ও ডিভাইস

একটি কম্পিউটারের ডিভাইসগুলোকে পাঁচটি ভাগে ভাগ করা যেতে পারে, যেমন—

ইনপুট ডিভাইস
আউটপুট ডিভাইস
প্রসেসিং ডিভাইস
মেমোরি ডিভাইস
বিশেষ ডিভাইস

### ৬.৪.১. ইনপুট ডিভাইস

কম্পিউটারে তথ্য, উপাত্ত এবং নির্দেশনা ইনপুট করার জন্য ব্যবহৃত কম্পিউটারের ডিভাইস বা অংশগুলোকে ইনপুট ডিভাইস বলা হয়। কীবোর্ড, মাউস, জয়স্টিক, স্ক্যানার, ডিজিটাল ক্যামেরা, মাইক্রোফোন ইত্যাদি ইনপুট ডিভাইসের উদাহরণ।

*কীবোর্ড*

মাউস

**কীবোর্ড :** কীবোর্ড এমন একটি ডিভাইস যাতে ১০৪ থেকে ১১০ সংখ্যক কী থাকে। এই কীগুলো অক্ষর এবং অঙ্ক টাইপ করার জন্য এবং কম্পিউটারে নির্দেশাবলি প্রদানের জন্য ব্যবহৃত হয়। একটি কীবোর্ড একটি কেবল (Cable) ব্যবহার করে একটি কম্পিউটারের মাদারবোর্ডের সঙ্গে সংযুক্ত থাকে।

**মাউস :** মাউস হলো উইন্ডোজ বা ম্যাকিনটোশ অপারেটিং সিস্টেম থাকা কম্পিউটারে নির্দেশনা প্রদানের জন্য বিকল্প বা সংশ্লিষ্ট সরঞ্জাম হিসাবে ব্যবহৃত একটি ডিভাইস। মাউসের ২ বা ৩ বোতাম আছে।

### ৬.৪.২. আউটপুট ডিভাইস

ব্যবহারকারীদেরকে ফলাফল প্রদর্শনের জন্য যে ডিভাইসগুলো ব্যবহার করা হয় তাকে আউটপুট ডিভাইস বলা হয়। মনিটর, প্রিন্টার, স্পিকার ও প্লটার হল আউটপুট ডিভাইসের উদাহরণ।

**মনিটর :** নির্দিষ্ট সরবরাহকৃত তথ্য এবং ডেটা প্রক্রিয়াকরণের ফলাফল একটি টিভির মতো ডিভাইসে টেক্সট, গ্রাফ বা ছবি ব্যবহার করে প্রদর্শিত হয় যাকে মনিটর বলে। মনিটর একটি ডেটা কেবল ব্যবহার করে কম্পিউটারের সিস্টেম

বোর্ডের সঙ্গে সংযুক্ত থাকে। কিছু মনিটরে একটি পৃথক পাওয়ার সংযোগের প্রয়োজন হয়।

*স্পিকার*

*মনিটর*

*প্রিন্টার*

প্রিন্টার কম্পিউটারের আউটপুট প্রিন্টার নামক একটি ডিভাইস ব্যবহার করে কাগজে প্রিন্ট করা হয়। প্রিন্টারটি একটি ডেটা কেবল ব্যবহার করে কম্পিউটারের সিস্টেম বোর্ডের সঙ্গে সংযুক্ত থাকে। অন্য আরেকটি কেবল ব্যবহার করে প্রিন্টারে পাওয়ার সরবরাহ করা হয়।

প্রিন্টার দুই প্রকার—ডট ম্যাট্রিক্স প্রিন্টার এবং লেজার প্রিন্টার। ডট ম্যাট্রিক্স প্রিন্টারের একটি 'হেড' রয়েছে যা একটি ফিতার উপর চাপ তৈরি করে। ফলে ফিতার কালি কাগজে অক্ষর, বিশেষ অক্ষর এবং অঙ্ক তৈরি করে। এপসন ডট ম্যাট্রিক্স প্রিন্টার এবং এপসন লাইন প্রিন্টার হলো ডট ম্যাট্রিক্স প্রিন্টারের উদাহরণ। লেজার প্রিন্টারে হেডের পরিবর্তে, একটি লেজার রশ্মি অক্ষর, বিশেষ অক্ষর এবং অঙ্ক তৈরি করতে ব্যবহৃত হয়। একটি লেজার প্রিন্টারে, ফিতার পরিবর্তে, একটি টোনার বা কার্টিজ ব্যবহার করা হয় যা কালি সরবরাহ করে থাকে। ইঙ্ক জেট প্রিন্টার এবং ক্যানন লেজার প্রিন্টার হলো লেজার প্রিন্টারের উদাহরণ।

স্পিকার : গান শোনা বা ভিডিও দেখার সময় শব্দ তৈরির জন্য একটি স্পিকার ব্যবহার করা হয়।

প্লটার : প্লটার, কম্পিউটার থেকে কাগজ ড্রয়িং ছাপানোর জন্য ব্যবহৃত হয়। প্লটার বড় ছবি, পোস্টার, ক্যালেন্ডার ও মানচিত্র মুদ্রণের জন্যও ব্যবহৃত হয়।

### ৬.৪.৩. প্রসেসিং ডিভাইস

কম্পিউটারে সরবরাহকৃত তথ্য, ডেটা ও নির্দেশাবলি প্রক্রিয়াকরণের জন্য ব্যবহৃত ডিভাইসগুলোকে প্রসেসিং ডিভাইস বলা হয়। সিপিইউ বা সেন্ট্রাল প্রসেসিং ইউনিট কম্পিউটারে ব্যবহৃত একটি প্রসেসিং ডিভাইস। এটি একটি কম্পিউটারের সমস্ত প্রক্রিয়াকরণ কার্যক্রম সম্পাদন করে। সিপিইউ মানুষের মস্তিষ্কের মতো। একটি কম্পিউটারের প্রক্রিয়াকরণের গতি এবং ক্ষমতা তার সিপিইউর ওপর নির্ভর করে।

১৯৭১ সালে, ইন্টেল কোম্পানি কম্পিউটারে ব্যবহারের জন্য একটি মাইক্রোপ্রসেসর আবিষ্কার করে। এটিকে ৮০০৮ মাইক্রোপ্রসেসর বলা হয়। তারপরে অ্যাপল ১৯৭৬ সালে এবং আইবিএম ১৯৮১ সালে মাইক্রোপ্রসেসর উৎপাদন করে।

একটি সিপিইউ-এর কার্যকারিতাগুলো নিচে বর্ণিত হয়েছে—

১. সিপিইউ কম্পিউটারের সমস্ত অংশে নিয়ন্ত্রণ এবং সময়-নির্ধারক সংকেত পাঠায়।
২. মেমোরি ও ইনপুট/আউটপুট ডিভাইসের মধ্যে ডেটা পাঠায় এবং গ্রহণ করে।
৩. মেমোরি থেকে ডেটা এবং নির্দেশাবলি গ্রহণ করে।
৪. নির্দেশাবলি ডিকোড করে।
৫. গাণিতিক এবং যৌক্তিক কার্যকলাপ সম্পাদন করে।
৬. কম্পিউটার মেমোরি থেকে প্রোগ্রাম চালায়।
৭. ইনপুট ও আউটপুট ডিভাইসের মধ্যে সমন্বয় করে।

স্থাপত্যের উপর ভিত্তি করে, একটি মাইক্রোপ্রসেসরকে সিস্‌ক প্রসেসর এবং রিস্‌ক প্রসেসরের মতো ২টি গ্রুপে ভাগ করা যায়।

সিস্‌ক বা কমপ্লেক্স ইন্সট্রাকশন সেট কম্পিউটার একটি মাইক্রোপ্রসেসর, যা মাইক্রোকোড ব্যবহার করে। মাইক্রোকোড কিছু নির্দেশাবলি (সফ্‌টওয়্যার প্রোগ্রাম) নিয়ে গঠিত, যা চিপের ভেতর থেকে কাজ করে। এই ধরনের মাইক্রোপ্রসেসর সফ্‌টওয়্যার দ্বারা চালিত হয়, তারা সাধারণত ধীর হয়. উদাহরণস্বরূপ সিস্‌ক মাইক্রোপ্রসেসরগুলো হলো ৮০৮৫, ৮০৮৬, ৮০৮৮, ৮০২৮৬, ৮০৩৮৬এসএক্স, ৮০৩৮৬ডিএক্স, ৮০৪৮৬এসএক্স, ৮০৪৮৬ডিএক্স, এবং ইন্টেলের পেন্টিয়াম, এএমডি-এর ৩৮৬ ডিএক্স, ৪৮৬ ডিএক্স এবং মটোরোলার ৬৮০০, ৬৮০০০, ৬৮০৪০।

রিস্‌ক বা রিডিউসড ইন্সট্রাকশন সেট কম্পিউটার হলো একটি মাইক্রোপ্রসেসর যাতে কম সংখ্যক নির্দেশনা সেট ব্যবহার করা হয়। এটি সফ্‌টওয়্যার-ভিত্তিক নয়, বরং হার্ডওয়্যার-ভিত্তিক এবং তা সিস্‌ক প্রসেসরের চেয়ে দ্রুত কাজ করে। ব্যাংকগুলো সাধারণত ডাটা সেন্টারে তাদের প্রধান ডাটাবেস সার্ভার হিসাবে রিস্‌ক প্রসেসর-ভিত্তিক কম্পিউটার ব্যবহার করে। ইউনিক্স সাধারণত এই ধরনের রিস্‌ক সার্ভারের অপারেটিং সিস্টেম হিসাবে ব্যবহৃত হয়। উদাহরণস্বরূপ, এআইএক্স আইবিএম রিস্‌ক সার্ভারের জন্য একটি অপারেটিং সিস্টেম, সান রিস্‌ক সার্ভারের

জন্য সান সোলারিস এবং এইচপি রিস্ক সার্ভারের জন্য এইচপি-ইউএক্স ব্যবহার করা হয়।

### ৬.৪.৪. মেমোরি ডিভাইস

মেমোরি ডিভাইসগুলো হল সেই ডিভাইস যেখানে কম্পিউটার ডেটা প্রক্রিয়াকরনের সময়, আগে বা পরে অস্থায়ীভাবে বা স্থায়ীভাবে ডেটা সংরক্ষণ করে থাকে। মেমোরি ডিভাইসগুলোকে ৩টি গ্রুপে শ্রেণিবদ্ধ করা যেতে পারে—প্রাথমিক বা প্রধান মেমোরি, ক্যাশ মেমোরি এবং সেকেন্ডারি বা অক্সিলিয়ারি মেমোরি।

### ৬.৪.৪.১. প্রাথমিক বা প্রধান মেমোরি

সিপিইউ এর সঙ্গে সরাসরি সংযুক্ত মেমোরিকে প্রাইমারি বা মেইন মেমোরি বলা হয়। এটি একটি প্রোগ্রাম কার্যকর করার সময় এর ডেটা, নির্দেশাবলি এবং ফলাফল সংরক্ষণ করতে ব্যবহৃত হয়। র‍্যাম এবং রম এই ধরনের মেমোরির উদাহরণ।

**র‍্যাম :** র‍্যাম-এর পূর্ণরূপ হলো র‍্যানডম এক্সেস মেমরি। কম্পিউটার প্রথমে ইনপুট ডিভাইস থেকে বা স্থায়ী স্টোরেজ থেকে সমস্ত প্রাসঙ্গিক ডেটা, প্রোগ্রাম ও নির্দেশাবলি গ্রহণ করে এবং পরবর্তীতে তা প্রক্রিয়াকরণের জন্য র‍্যামে লিখে। র‍্যাম-এর নিম্নলিখিত বৈশিষ্ট্য রয়েছে—

১. র‍্যাম সবসময় ভলেটাইল।
২. এটি এমন একটি মেমোরি যেখানে লেখা যায় ও যা থেকে পড়াও যায়।
৩. প্রক্রিয়াকরণের সময় তথ্য র‍্যামে অবস্থান করে।
৪. বৈদ্যুতিক পাওয়ার বন্ধ হয়ে গেলে র‍্যাম থেকে সমস্ত তথ্য মুছে ফেলা হয়।

**রম** : রমের অর্থ রিড অনলি মেমোরি। রমে BIOS (বেসিক ইনপুট আউটপুট সিস্টেম) নামক একটি প্রোগ্রাম ধারণ করে। একটি কম্পিউটারের সমস্ত ডিভাইসের তালিকা, অবস্থান ও স্পেসিফিকেশন BIOS-এ রেকর্ড করা হয়। স্টার্টআপের সময় কম্পিউটার BIOS-এর সাহায্যে সমস্ত ডিভাইস চিনতে পারে। একটি রমের বৈশিষ্ট্য নিম্নরূপ—

*র‍্যাম*

১. রম একটি স্থায়ী প্রধান মেমোরি।
২. রম-এর তথ্য শুধু পড়া যায়, কিন্তু পরিবর্তন করা যায় না।
৩. কম্পিউটার চালু করার জন্য প্রয়োজনীয় প্রোগ্রামগুলো রমে স্থায়ীভাবে সংরক্ষণ করা হয়।
৪. পাওয়ার চলে গেলে, রম-এর তথ্য মুছে যায় না।

### ৬.৪.৪.২. সেকেন্ডারি বা অক্সিলিয়ারি মেমোরি

ব্যবহারকারীর প্রোগ্রাম এবং তথ্য স্থায়ীভাবে সংরক্ষণ করার জন্য যে মেমোরি ব্যবহার করা হয় তাকে সেকেন্ডারি বা অক্সিলিয়ারি মেমোরি বলে। উদাহরণ হলো ফ্লপি ডিস্ক, হার্ড ডিস্ক, কমপ্যাক্ট ডিস্ক, ম্যাগনেটিক টেপ, পেন ড্রাইভ ইত্যাদি।

**ফ্লপি ডিস্ক :** একটি পাতলা প্লাস্টিকের শিটে চৌম্বকীয় স্তর রেখে যে হালকা ও ছোট ডিস্ক তৈরি হয় তাকে ফ্লপি ডিস্ক বলে। তথ্য এবং প্রোগ্রাম একটি ফ্লপি ডিস্কে সংরক্ষণ করা হয়। সাধারণত এক কম্পিউটার থেকে অন্য কম্পিউটারে তথ্য স্থানান্তর করতে ফ্লপি ডিস্ক ব্যবহার করা হয়। ফ্লপি ডিস্ক দুটি আকারের—৩.৫ ‘এবং ৫.২৫’। একটি ফ্লপি ডিস্ক থেকে তথ্য পড়তে এবং তাতে লিখতে ব্যবহৃত ডিভাইসটিকে ফ্লপি ড্রাইভ বলা হয়। ফ্লপি ড্রাইভ দুটি আকারে পাওয়া যায় - ৩.৫ ‘এবং ৫.২৫’।

৩.৫ ‘ফ্লপি ডিস্কের ক্ষমতা হলো ১.৪৪ এমবি এবং ৫.২৫’ ফ্লপি ড্রাইভের ক্ষমতা হলো ৩৬০ কেবি।

পেন ড্রাইভ আবিষ্কারের কারণে ফ্লপি ড্রাইভের ব্যবহার অপ্রিয় হয়ে উঠেছে।

হার্ড ডিস্ক : একটি হার্ড ডিস্ক স্ক্রু এবং ডেটা ও পাওয়ার ক্যাবল ব্যবহার করে কম্পিউটার বক্সের ভেতরে সংযুক্ত থাকে এবং ফ্লপি ডিস্কের তুলনায় এর ক্ষমতা ও গতি অনেক বেশি। ডেটা এবং প্রোগ্রামগুলো সাধারণত হার্ড ডিস্কে সংরক্ষণ করা হয়। হার্ডডিস্ক ব্যবহারের জন্য কম্পিউটারে কোনো ড্রাইভের প্রয়োজন নেই। বাজারে বিভিন্ন ক্ষমতার হার্ড ডিস্ক পাওয়া যায় যেমন ২৫০ জিবি হার্ডডিস্ক, ৫০০ জিবি হার্ডডিস্ক ইত্যাদি।

**কমপ্যাক্ট ডিস্ক :** কমপ্যাক্ট ডিস্ককে সংক্ষেপে সিডি বলা হয়। সিডি সাধারণত ডেটা, প্রোগ্রাম, গান, গেম, ভিডিও ইত্যাদি রেকর্ডিং বা সংরক্ষণের জন্য এবং এক কম্পিউটার থেকে অন্য কম্পিউটারে ডেটা স্থানান্তর করার জন্য ব্যবহৃত হয়। কিছু সিডি থেকে শুধু তথ্য পড়া যায়। এতে তথ্য পরিবর্তন করা যায় না। এছাড়াও এই সিডিগুলোতে নতুন তথ্য যোগ করা যায় না। এই সিডিগুলোকে বলা হয় সিডি-রম (রিড অনলি মেমরি)। কম্পিউটারের সঙ্গে সংযুক্ত এবং সিডি থেকে তথ্য পড়ার

জন্য ব্যবহৃত ড্রাইভকে সিডি ড্রাইভ বলে। কিছু সিডি আছে যাতে পড়তে, পরিবর্তন করতে এবং তথ্য যোগ করতে পারা যায়। এই সিডিগুলোকে বলা হয় রি-রাইটেবল সিডি (সিডি-আরডব্লিউ)। সিডি-আরডব্লিউতে তথ্য পড়া, পরিবর্তন এবং যোগ করার জন্য কম্পিউটারের সঙ্গে একটি ডিভাইস সংযুক্ত থাকে যাকে সিডি রাইটার বলা হয়। একটি সিডি একটি বৃত্তাকার ডিস্কের মতো যার ব্যাস ৪.৭৫'। একটি সিডির ক্ষমতা ৬৫০ এমবি।

*কমপ্যাক্ট ডিস্ক*

*পেন ড্রাইভ*

**ম্যাগনেটিক টেপ :** ম্যাগনেটিক টেপ হলো একটি প্লাস্টিকের রিল, যা আয়রন অক্সাইড দিয়ে আবৃত এবং একটি ক্যাসেটে মোড়ানো। ম্যাগনেটিক টেপ হার্ড ডিস্ক থেকে টেপে দরকারি ডেটা ব্যাকআপ করার জন্য ব্যবহার করা হয়। এটি নিশ্চিত করে যে হার্ডডিস্কের ক্ষতির ক্ষেত্রে ডেটা পাওয়া যাবে। হার্ডডিস্ক থেকে ম্যাগনেটিক টেপে ডাটা ডুপ্লিকেশন করাকে ব্যাকআপ বলে। ব্যাংক প্রতিদিন গ্রাহকের ডেটার একটি ব্যাকআপ কপি তৈরি করে। টেপ ড্রাইভ একটি ডিভাইস, যা একটি ডেটা কেবল ব্যবহার করে কম্পিউটারের সঙ্গে সংযুক্ত থাকে এবং কম্পিউটারের হার্ড ডিস্ক থেকে একটি ম্যাগনেটিক টেপে ডেটা কপি করতে সাহায্য করে।

**পেন ড্রাইভ :** পেন ড্রাইভ একটি ডেটা স্টোরেজ ডিভাইস, যা দেখতে একটি ফ্লপি ডিস্কের চেয়ে অনেক ছোট, কিন্তু ২ জিবি, ৪ জিবি, ৮ জিবি এবং ২৫৬ জিবি পর্যন্ত ডেটা সংরক্ষণ করতে পারে। চলন্ত পার্টস না থাকার কারণে এগুলো আরও টেকসই এবং নির্ভরযোগ্য। একটি পেন ড্রাইভকে একটি ইউএসবি ফ্লাশ ড্রাইভও বলা হয়, কারণ এটি এক প্রান্তে একটি ইউএসবি (ইউনিভার্সাল সিরিয়াল বাস) কানেক্টর সংযুক্ত থাকে। কানেক্টরটি একটি কম্পিউটারে ইউএসবি পোর্টে ঢোকানো হয় এবং ফাইল বা ডেটা পেনড্রাইভ থেকে/এ কপি করা যায়।

### ৬.৪.৪.৩. ক্যাশ মেমোরি (Cache Memory)

প্রক্রিয়াকরণের গতি বাড়ানোর জন্য সিপিইউ বা প্রধান মেমোরির সঙ্গে রাখা একটি বিশেষ মেমোরিকে ক্যাশ মেমোরি বলা হয়। ক্যাশ মেমরি দুটি প্রকারে শ্রেণিবদ্ধ করা যেতে পারে—অভ্যন্তরীণ ক্যাশ এবং বাহ্যিক ক্যাশ। অভ্যন্তরীণ ক্যাশ মাইক্রোপ্রসেসরের ভেতরে স্থাপন করা হয় যেখানে বাহ্যিক ক্যাশ মাদারবোর্ডে আইসি (ইন্টিগ্রেটেড সার্কিট) হিসাবে স্থাপন করা হয়।

### ৬.৪.৫. বিশেষ ডিভাইস

ইনপুট, আউটপুট এবং মেমোরি ডিভাইসগুলোকে আন্তঃসংযোগ করতে ব্যবহৃত ডিভাইসগুলোকে স্পেশাল ডিভাইস বলে। সিস্টেম বক্স, মাদার বোর্ড এবং পাওয়ার সাপ্লাই ইউনিট স্পেশাল ডিভাইসের উদাহরণ।

*সিস্টেম ইউনিট*

*মাদারবোর্ড ও পাওয়ার ইউনিট*

**সিস্টেম বক্স :** একটি বাক্স যেখানে মাদারবোর্ড, হার্ডডিস্ক, ফ্লপি ডিস্ক, সিডি ড্রাইভ এবং পাওয়ার সাপ্লাই ইউনিট স্ক্রু এবং তারের সাহায্যে সংযুক্ত থাকে, তাকে সিস্টেম বক্স বলে। অনেকে ভুলভাবে সিস্টেম বক্সকে সিপিইউ বলে। একটি সিস্টেম বক্স, একটি মনিটর, একটি কীবোর্ড এবং একটি মাউসসহ সমস্ত প্রয়োজনীয় ডিভাইসকে একত্রে একটি কম্পিউটার বলে।

**মাদার বোর্ড :** একটি যন্ত্র যা স্ক্রু ব্যবহার করে সিস্টেম বক্সের সঙ্গে সংযুক্ত থাকে এবং যার ওপর বিভিন্ন স্লট থাকে যার উপর সিপিইউ (প্রসেসর), রম ও র‍্যাম

সরাসরি সংযুক্ত থাকে, তাকে মাদার বোর্ড বলে। মাদারবোর্ডে বিভিন্ন পোর্টও রয়েছে, যার সঙ্গে কীবোর্ড, মাউস, মনিটর, ফ্লপি ড্রাইভ, সিডি ড্রাইভ ও প্রিন্টার কেবল ব্যবহার করে সংযুক্ত থাকে। মাদারবোর্ডের ভেতরে হাজার হাজার তার রয়েছে যা অভ্যন্তরীণভাবে বিভিন্ন ডিভাইসকে সংযুক্ত করে এবং একটি ডিভাইস থেকে অন্য ডিভাইসে ডেটা ও সংকেত বহন করে। এই তারের সিস্টেমকে বাস সিস্টেম বলা হয়।

**পাওয়ার সাপ্লাই ইউনিট :** একটি পাওয়ার সাপ্লাই ইউনিট হলো সেই কম্পোনেন্ট যা কম্পিউটারের অন্যান্য কম্পোনেন্টে পাওয়ার সরবরাহ করে। আরও বিশেষভাবে বলতে গেলে, একটি পাওয়ার সাপ্লাই ইউনিট সাধারণত অল্টারনেটিং কারেন্টকে (এসি) ডাইরেক্ট কারেন্টে (ডিসি) রূপান্তর করার জন্য তৈরি করা হয়, যা কম্পিউটারের বিভিন্ন অংশের জন্য বিশেষভাবে প্রয়োজনীয়।

**ইউপিএস :** ইউপিএস মানে নিরবচ্ছিন্ন বিদ্যুৎ সরবরাহ। ইউপিএস হলো একটি বৈদ্যুতিক যন্ত্রপাতি যা ইনপুট পাওয়ার সোর্স ব্যর্থ হলে কম্পিউটারে জরুরি বিদ্যুৎ সরবরাহ করে, এভাবে কম্পিউটারকে হঠাৎ বন্ধ হওয়া থেকে রক্ষা করে। ইউপিএস দুই ধরনের হতে পারে—অনলাইন ইউপিএস এবং অফলাইন ইউপিএস। অনলাইন ইউপিএস-এ শূন্য ট্রান্সফার টাইম থাকে এবং এটি সার্ভারের সঙ্গে ব্যবহৃত হয়। কিন্তু একটি অফলাইন ইউপিএস-এর ট্রান্সফার টাইম ৫-১০ সেকেন্ড থাকে। উভয় প্রকারের ইউপিএসই কম্পিউটারকে পাওয়ার ব্যর্থতার ক্ষেত্রে বন্ধ হওয়া থেকে রক্ষা করতে পারে, তবে অনলাইন ইউপিএস, উপরন্তু, বিদ্যুৎ ওঠানামার কারণে ডেটা ক্ষতিগ্রস্ত হওয়া থেকে রক্ষা করতে পারে, কারণ এই ধরনের ইউপিএস-এর মধ্যে বিদ্যুৎ থেকে ব্যাটারিতে সুইচ করার জন্য কোনও ট্রান্সফার টাইমের প্রয়োজন হয় না।

ভোল্টেজ স্টেবিলাইজার : একটি ভোল্টেজ স্টেবিলাইজার একটি বৈদ্যুতিক নিয়ন্ত্রক, যা ইনপুট ভোল্টেজের তারতম্য নির্বিশেষে স্বয়ংক্রিয়ভাবে সবসময় একই পরিমাণের ভোল্টেজ আউটপুট হিসাবে বজায় রাখার জন্য ডিজাইন করা হয়েছে। ভোল্টেজ স্ট্যাবিলাইজারগুলো কম্পিউটার সিস্টেমের সঙ্গে ব্যবহৃত হয়, যাতে ভোল্টেজের আকস্মিক ওঠানামা থেকে কম্পিউটারকে রক্ষা করতে পারে।

## ৭. কম্পিউটার সফটওয়্যার

কম্পিউটার একটি মেশিন, যা নিজে কাজ করতে পারে না। কম্পিউটার চালু করতে এবং অপারেটিভ করতে একটি কম্পিউটার প্রোগ্রাম প্রয়োজন। কম্পিউটারকে অপারেটিভ করার পর, একটি নির্দিষ্ট কাজ সম্পাদনের জন্য নির্দিষ্ট প্রোগ্রামের আরেকটি সেট প্রয়োজন। এই ধরনের প্রোগ্রামগুলো সম্মিলিতভাবে কম্পিউটার সফ্টওয়্যার হিসাবে পরিচিত। কম্পিউটার সফটওয়্যারকে দুই ভাগে ভাগ করা যায়—সিস্টেম সফটওয়্যার এবং অ্যাপ্লিকেশন সফটওয়্যার।

### ৭.১. সিস্টেম সফটওয়্যার

কম্পিউটারকে চালু করতে যে সফটওয়্যার ব্যবহার করা হয় তাকে সিস্টেম সফ্টওয়্যার বলে। অন্যদিকে যখন অ্যাপ্লিকেশন সফ্টওয়্যার কম্পিউটার সিস্টেমের একটি ডিভাইসকে কিছু করার নির্দেশ দেয়, তখন সিস্টেম সফ্টওয়্যার প্রথমে নির্দেশটিকে এমন একটি ভাষায় অনুবাদ করে যা ডিভাইসটি সহজেই বুঝতে পারে। ডিভাইসগুলো সেই অনুযায়ী কাজ করে। কাজেই সিস্টেম সফ্টওয়্যার, কম্পিউটার হার্ডওয়্যার এবং অ্যাপ্লিকেশন সফ্টওয়্যারের মাঝখানে অবস্থান করে। অপারেটিং সিস্টেমগুলো হলো সিস্টেম সফ্টওয়্যারের উদাহরণ।

অপারেটিং সিস্টেমটি প্রথম ১৯৬০-এর দশকে মেইনফ্রেম কম্পিউটারের জন্য তৈরি করা হয়েছিল। পরবর্তীতে ম্যাকিনটোশ, ডিস্ক অপারেটিং সিস্টেম (ডস), ইউনিক্স এবং উইন্ডোজের মতো বিভিন্ন অপারেটিং সিস্টেম তৈরি করা হয়। মার্কিন যুক্তরাষ্ট্রের মাইক্রোসফ্ট কোম্পানি ডস ও উইন্ডোজ অপারেটিং সিস্টেমের প্রস্তুতকারী। একটি অপারেটিং সিস্টেমের কার্যকারিতা নিম্নে উল্লেখ করা হয়েছে—

১. কম্পিউটারকে সক্রিয় এবং ব্যবহার উপযোগী করা।
২. হার্ডওয়্যার ও অ্যাপ্লিকেশন সফ্টওয়্যারের মধ্যে যোগাযোগ করা।
৩. একজন ব্যবহারকারীর নির্দেশ গ্রহণ এবং কার্যকর করা।
৪. প্রধান মেমোরিতে একটি প্রোগ্রাম আনা এবং এটি প্রক্রিয়া করা।
৫. ডিস্ক থেকে ডেটা পড়া বা ডিস্কে ডেটা লেখা এবং সংরক্ষণ প্রক্রিয়া নিয়ন্ত্রণ করা।

### ৭.২. অ্যাপ্লিকেশন সফ্টওয়্যার

একটি কম্পিউটার ব্যবহার করে একটি নির্দিষ্ট কাজ সম্পাদনের জন্য ব্যবহৃত একটি প্রোগ্রামকে অ্যাপ্লিকেশন সফটওয়্যার বলে। উদাহরণস্বরূপ, ওয়ার্ড স্টার, ওয়ার্ড পারফেক্ট এবং এমএস ওয়ার্ড, টাইপিং বা বর্ণ প্রক্রিয়াকরণের জন্য ব্যবহৃত হয়; লোটাস ১-২-৩, কোয়াট্রো প্রো, এমএস, এবং এক্সেল গণনা বা স্প্রেডশিট বিশ্লেষণের জন্য ব্যবহার করা হয়; নেটস্কেপ নেভিগেটর, ইন্টারনেট এক্সপ্লোরার, গুগল ক্রোম এবং ফায়ারফক্স ওয়েব ব্রাউজিংয়ের জন্য ব্যবহৃত হয়; আউট লুক, মেসেঞ্জার এবং ইউডোরা ই-মেইল চেকিং এর জন্য ব্যবহার করা হয়, পাওয়ারপয়েন্ট ব্যবহার করা হয় উপস্থাপনার জন্য; অটো ক্যাড ইঞ্জিনিয়ারিং ড্রয়িং-এর জন্য ব্যবহৃত হয়; এসপিএসএস পরিসংখ্যানগত বিশ্লেষণের জন্য ব্যবহৃত হয়;

ডেটা ম্যানিপুলেশন এবং স্টোরেজের জন্য অ্যাক্সেস, এসকিউএল সার্ভার এবং ওরাকল ব্যবহার করা হয়। এই সফটওয়্যারগুলো বিভিন্ন কোম্পানি তৈরি করে বাজারে বাণিজ্যিকভাবে বিক্রি করার জন্য। ব্যবহারকারীরা এগুলো কিনে বাসায় ও অফিসে ব্যবহার করেন। এই কারণে, তাদের জেনারেল পারপাস অ্যাপ্লিকেশন সফ্টওয়্যার বলা হয়।

প্রোগ্রামাররা একটি নির্দিষ্ট প্রতিষ্ঠানের একটি নির্দিষ্ট কার্যকলাপের জন্য অ্যাপ্লিকেশন সফ্টওয়্যার তৈরি করে। এগুলোকে বলা হয় অ্যাপ্লিকেশন-স্পেসিফিক প্রোগ্রাম। উদাহরণস্বরূপ, প্রোগ্রামারদের একটি গ্রুপ বা একটি কোম্পানি একটি ব্যাংকের জন্য তার গ্রাহকদের লেনদেন রেকর্ড করার জন্য একটি প্রোগ্রাম তৈরি করতে পারে এবং শেষে, ব্যালেন্স শিট ও ইনকাম স্টেটমেন্টের মতো রিপোর্ট তৈরি করতে পারে। একটি ব্যাংকের জন্য লিখিত প্রোগ্রাম অন্য ব্যাংকের প্রয়োজনীয়তার সঙ্গে খাপ নাও খেতে পারে, কারণ বিভিন্ন ব্যাংকের জন্য লেনদেনের নিয়ম আলাদা হতে পারে।

## ৭.৩. প্রোগ্রামিং ভাষা (Programming Language)

যে প্রোগ্রামটি ব্যবহার করে একটি জেনারাল পারপাস প্রোগ্রাম বা একটি অ্যাপ্লিকেশন স্পেসিফিক প্রোগ্রাম লেখা হয় তাকে প্রোগ্রামিং ভাষা বলে। বড় কোম্পানিগুলো বাণিজ্যিকভাবে বিক্রি করার জন্য প্রোগ্রামিং ভাষা তৈরি করে। প্রোগ্রামাররা এই প্রোগ্রামিং ল্যাঙ্গুয়েজগুলো কেনে এবং একটি জেনারাল-পারপাস বা অ্যাপ্লিকেশন-স্পেসিফিক প্রোগ্রাম লিখতে তাদের ব্যবহার করে। সাধারণত ব্যবহৃত প্রোগ্রামিং ভাষা হলো—

১. সি/সি++
২. জাভা
৩. এসেম্বলি ভাষা
৪. কোবল
৫. ফোরট্রান
৬. বেসিক/বেসিকা/কিউ-বেসিক/কুইক বেসিক
৭. ভিজ্যুয়াল বেসিক
৮. ডট নেট
৯. এইচটিএমএল
১০. ফক্সপ্রো / ফক্সবেস / ডিবেস

প্রোগ্রামিং ভাষাকে তিন প্রকারে ভাগ করা যায়—

১. লো-লেভেল ভাষা
২. হাই-লেভেল ভাষা
৩. অবজেক্ট ওরিয়েন্টেড ভাষা

### ৭.৩.১. লো-লেভেল ভাষা (Low-level Language)

লো-লেভেল ভাষাগুলো এমন ভাষা, যেখানে কম্পিউটার প্রোগ্রামগুলো মেশিন কোড (বাইনারি বা হেক্সাডেসিমেল কোড) বা মেমোনিক কোড ব্যবহার করে লেখা হয়। লো-লেভেল ভাষা দুটি কম্পিউটার ভাষা নিয়ে গঠিত—মেশিন ভাষা ও অ্যাসেম্বলি ভাষা।

**মেশিন ভাষা :** কম্পিউটারের বিকাশের প্রাথমিক পর্যায়ে, প্রোগ্রামাররা কম্পিউটার প্রোগ্রাম লেখার জন্য মেশিন কোড অর্থাৎ বাইনারি এবং হেক্সাডেসিমেল কোড ব্যবহার করত। এই কম্পিউটার প্রোগ্রামগুলো যেগুলো নির্দিষ্ট ব্যবহারকারীর প্রোগ্রামগুলো লিখতে মেশিন কোড ব্যবহার করে তাকে মেশিন ভাষা বলা হয়। মেশিনের ভাষা খুব দ্রুত এবং দক্ষতার সঙ্গে কার্যকর হয়। তবে যদি নির্দিষ্ট প্রোগ্রামার একটি নির্দিষ্ট কম্পিউটারের জন্য একটি মেশিন ভাষা ব্যবহার করে একটি প্রোগ্রাম লিখেন তবে এটি অন্য কম্পিউটারে চালানো যাবে না। এই ধরনের কম্পিউটার প্রোগ্রাম লেখা, পড়া এবং পরিবর্তন করা খুবই জটিল এবং সময়সাপেক্ষ। এই সমস্যা সমাধানের জন্য, কম্পিউটার প্রোগ্রামগুলো আরও আরামদায়ক লেখার জন্য অ্যাসেম্বলি ভাষা তৈরি করা হয়েছিল।

**অ্যাসেম্বলি ল্যাঙ্গুয়েজ :** অ্যাসেম্বলি ল্যাঙ্গুয়েজে, বাইনারি এবং হেক্সাডেসিমেল কোডের মতো মেশিন কোডের পরিবর্তে মেমোনিক কোড ব্যবহার করা হয়। উদাহরণস্বরূপ, অ্যাসেম্বলি ল্যাঙ্গুয়েজ প্রোগ্রামগুলো একটি বিয়োগ ক্রিয়া সম্পাদন করতে সাব (SUB) ব্যবহার করে। এ জন্য অ্যাসেম্বলি ভাষাকে সিম্বলিক ভাষাও বলা হয়। একটি অপারেটিং সিস্টেম, একটি গেম, বা একটি হাই-লেভেল ভাষা তৈরির জন্য, সাধারণত অ্যাসেম্বলি ভাষা ব্যবহার করা হয়।

### ৭.৩.২. হাই-লেভেল ভাষা (High-level Language)

একটি হাই-লেভেল ভাষা (অ্যাসেম্বলি ভাষা ব্যবহার করে তৈরি) খুবই ব্যবহারকারী-বান্ধব। এর সিনট্যাক্সগুলো ইংরেজি ভাষার সঙ্গে খুব মিল। কম্পিউটার প্রোগ্রামাররা একটি হাই-লেভেল ভাষা সাধারনত একটি অ্যাপ্লিকেশন-স্পেসিফিক কম্পিউটার প্রোগ্রাম তৈরি করতে ব্যবহার করে। নিম্নে হাই-লেভেল ভাষার উদাহরণ দেওয়া হলো—

১. কোবল (Common Business Oriented Language)
২. বেসিক (Beginners All-Purpose Symbolic Instruction Code)

৩. ফরট্রান (Formula Translator)
৪. সি (C)
৫. প্যাসকেল (Pascal)

### ৭.৩.৩. অবজেক্ট ওরিয়েন্টেড ল্যাঙ্গুয়েজ (Object Oriented Language)

অবজেক্ট ওরিয়েন্টেড ল্যাঙ্গুয়েজ হলো এমন একটি ভাষা, যা প্রোগ্রামিং কোড এবং ডেটাকে একটি 'অবজেক্ট' নামক প্রোগ্রামিং কোডের সেটে একত্রিত করে থাকে। অবজেক্টটি পুরো প্রোগ্রাম জুড়ে বারবার ব্যবহার করা যেতে পারে। অবজেক্ট ওরিয়েন্টেড ল্যাঙ্গুয়েজ ব্যবহার করে কম্পিউটার প্রোগ্রাম লেখার কৌশলকে বলা হয় অবজেক্ট ওরিয়েন্টেড প্রোগ্রামিং বা ওওপি। একটি ওওপি-এর নিম্নলিখিত তিনটি বৈশিষ্ট্য আছে—

**ক. পলিমরফিজম (Polymorphism)**

পলিমরফিজম মানে বিভিন্ন অবজেক্ট একই বার্তায় স্বতন্ত্রভাবে সাড়া দেয়। উদাহরণস্বরূপ, যখন আমরা একটি বিড়াল নামক অবজেক্ট, একটি কুকুর নামক অবজেক্ট এবং একটি গরু নামক অবজেক্ট-কে 'কথা বলুন' বার্তাটি পাঠাই, তখন প্রত্যেকে যথাযথভাবে প্রতিক্রিয়া জানায়। বিড়াল চিৎকার করে, কুকুর ঘেউ ঘেউ করে, আর গরু ডাক দিয়ে।

**খ. উল্টরাধিকার (Inheritance)**

উত্তরাধিকার মানে ভাষা আমাদের বিদ্যমান অবজেক্টকে প্রসারিত বা উন্নত করার ক্ষমতা দেয়। প্যারেন্ট অবজেক্ট থেকে তৈরি চাইল্ড অবজেক্ট, প্যারেন্ট অবজেক্টের সমস্ত বৈশিষ্ট্য পাবে এবং এর নিজস্ব কিছু বৈশিষ্ট্যও থাকতে পারে।

**গ. এনক্যাপসুলেশন (Encapsulation)**

এনক্যাপসুলেশন মানে ভেরিয়েবলের জন্য ডেটা এবং নির্দেশাবলি একসঙ্গে মোড়ানো হয় এবং একটি ইউনিট হিসাবে বিবেচিত হয়। এই ভেরিয়েবলের ব্লুপ্রিন্টগুলোকে বলা হয় ক্লাস এবং ইউনিটগুলোকে অবজেক্ট বলা হয়
অবজেক্ট-ওরিয়েন্টেড ভাষার উদাহরণ হল সি$^{++}$ এবং জাভা।

### ৭.৪. ডাটাবেস ম্যানেজমেন্ট সিস্টেম (Database Management System)

একটি নির্দিষ্ট উদ্দেশ্যে একটি কম্পিউটার প্রোগ্রাম লিখতে প্রোগ্রামিং ভাষা ব্যবহার করা হয়। এই ধরনের একটি কম্পিউটার প্রোগ্রামে, কিছু ইনপুট স্ক্রিন থাকতে পারে যার মাধ্যমে ব্যবহারকারীরা কম্পিউটার সিস্টেমে ডেটা ইনপুট করে। এই তথ্যগুলো কম্পিউটার সিস্টেমে আরও ব্যবহারের জন্য বা পরবর্তীতে প্রতিবেদন তৈরির জন্য সংরক্ষণ করা হয়। সহজে পুনরুদ্ধারযোগ্য পদ্ধতিতে কম্পিউটার সিস্টেমে ডেটা সংরক্ষণের জন্য, ডেটাবেস ব্যবহার করা হয়। একটি ডাটাবেস হল একটি কম্পিউটার প্রোগ্রাম, যা ডেটা সংরক্ষণ এবং ম্যানিপুলেট করতে ব্যবহৃত হয়। একটি ডাটাবেসে, ডেটা সারি ও কলাম আকারে রাখা হয়। যা নিচে দেখানো হলো—

| সারি /কলাম | অ্যাকাউন্ট নং | গ্রাহকের নাম | অ্যাকাউন্ট ব্যালেন্স |
|---|---|---|---|
| ১ | S১০১ | অর্নব আলিনুর | ৫০০০.০০ |
| ২ | S১০২ | আবরার রহমান | ৩০১০.০০ |
| ৩ | C ১০১ | আমিনুল ইসলাম | ২৫০৫.০০ |
| ৪ | C ১০২ | রাইয়ান ইসলাম | ৪০১৭.০০ |

উপরের উদাহরণে, যে ফাইলে এই তথ্যগুলো সংরক্ষণ করা হবে তাকে ডাটাবেস টেবিল বলা হয়। এক বা একাধিক ডাটাবেস টেবিল একসঙ্গে একটি ডাটাবেস তৈরি করে। ডাটাবেস এবং এর সমস্ত টেবিলের আলাদা আলাদা নাম রয়েছে। সমস্ত টেবিলের সারি এবং কলাম আছে। উপরের উদাহরণে, ৪টি সারি এবং ৩টি কলাম রয়েছে।

একটি ডাটাবেসের জন্য কিছু নির্দিষ্ট কমান্ড আছে যেমন, টেবিল তৈরি/সংশোধন/মুছে ফেলার জন্য, টেবিলে সারি যোগ করতে এবং টেবিল থেকে সারি পড়তে/পরিবর্তন/মুছে ফেলতে। এই কমান্ডগুলোকে ডেটা ডেসক্রিপশন ল্যাঙ্গুয়েজ (ডিডিএল) এবং ডেটা ম্যানিপুলেশন ল্যাঙ্গুয়েজ (ডিএমএল) বলা হয়।

ডাটাবেস ম্যানেজমেন্ট সিস্টেম (ডিবিএমএস) হলো এমন একটি সিস্টেম যা শুধু ডেটা সঞ্চয় করে না, কিন্তু ব্যবহারকারীদের জন্য ডেটা ডেসক্রিপশন ল্যাঙ্গুয়েজ (ডিডিএল) এবং ডেটা ম্যানিপুলেশন ল্যাঙ্গুয়েজ (ডিএমএল) প্রদান করে যাতে সহজেই ডেটা সেইভ করা এবং ডেটা ম্যানিপুলেশন করা যায়।

গ্রাহাম টেলরের মতে, ডিবিএমএস হল প্রোগ্রামের একটি জেনারাল সেট যা বিভিন্ন ব্যবহারকারী অ্যাপ্লিকেশন প্রোগ্রাম এবং ডাটাবেসের মধ্যে লিঙ্ক তৈরি করার জন্য ব্যবহার করে থাকে। এটি অ্যাক্সেস নিয়ন্ত্রণ করে (যারা এটি ব্যবহার করতে পারে) এবং ডেটার স্বাধীনতা, অখণ্ডতা ও নিরাপত্তা নিশ্চিত করে থাকে।

ডিবিএমএস একটি ব্যাংকের জন্য খুব দরকারি। ব্যালেন্স ও লেনদেনগুলো ডিবিএমএস-এ রেকর্ড করা হয়। ওরাকল, ডিবি ২ এবং এসকিউএল সার্ভার- এই তিনটি ব্যাংকে ব্যাপকভাবে ব্যবহৃত ডিবিএমএস।

যে কর্মকর্তা একটি ডিবিএমএস পরিকল্পনা, সংগঠিত এবং নিয়ন্ত্রণের জন্য নিযুক্ত থাকেন তাকে ডেটাবেস অ্যাডমিনিস্ট্রেটর (ডিবিএ) বলা হয়। একজন ডিবিএ, ডিবিএমএসে ডেটার নিরাপত্তা এবং প্রাপ্যতার জন্য দায়ী। যদি কোনো কারণে ডাটাবেস ক্র্যাশ হয়ে যায়, তাহলে ডিবিএ-এর দায়িত্ব হচ্ছে ডাটাগুলোকে

সবচেয়ে কম সময়ের মধ্যে পুনরুদ্ধার করা। এই কারণে, ডিবিএ সবসময় (সাধারণত দিনের শেষে) ডাটাবেসের একটি কপি একটি টেপ কার্টিজ এবং অন্য একটি কম্পিউটার সিস্টেমে রাখেন। একে বলা হয় ডাটাবেসের ব্যাকআপ নেওয়া।

## ৮ ইন্টারনেট এবং এ সম্পর্কিত পরিভাষা

### ৮.১. ইন্টারনেট (Internet)

ইন্টারনেট হলো আন্তঃসংযুক্ত কম্পিউটার নেটওয়ার্কগুলোর একটি বিশ্বব্যাপী সিস্টেম যা বিশ্বব্যাপী কোটি কোটি ব্যবহারকারীর পরিষেবা দেওয়ার জন্য স্ট্যান্ডার্ড ইন্টারনেট প্রোটোকল স্যুট (টিসিপি/আইপি) ব্যবহার করে। এটি নেটওয়ার্কসমূহের একটি নেটওয়ার্ক যা স্থানীয় থেকে বিশ্বব্যাপী বিস্তৃত, যা লক্ষ লক্ষ ব্যক্তিগত, পাবলিক, একাডেমিক, ব্যবসায়িক ও সরকারি নেটওয়ার্ক নিয়ে গঠিত, যা ইলেকট্রনিক ও অপটিক্যাল নেটওয়ার্কিং প্রযুক্তি ব্যবহার করে একের সঙ্গে অন্যটি সংযুক্ত। ইন্টারনেট বিভিন্ন তথ্য সংস্থান ও পরিষেবা বহন করে, যেমন ওয়ার্ল্ড ওয়াইড ওয়েব (www) এর ইন্টারলিঙ্কড হাইপারটেক্সট ডকুমেন্ট ও ইলেকট্রনিক মেল সমর্থন করার জন্য পরিকাঠামো।

টেলিফোন, মিউজিক, ফিল্ম এবং টেলিভিশনসহ বেশিরভাগ ঐতিহ্যবাহী যোগাযোগ মাধ্যম ইন্টারনেটের মাধ্যমে নতুন আকার ধারণ করেছে। সংবাদপত্র, বই এবং অন্যান্য মুদ্রণ প্রকাশনাকে ওয়েব সাইট ও ব্লগিংয়ের সঙ্গে খাপ খাইয়ে নিতে হচ্ছে। ইন্টারনেট তাৎক্ষণিক বার্তাপ্রেরণ, ইন্টারনেট ফোরাম ও সামাজিক নেটওয়ার্কিংয়ের মাধ্যমে মানুষের মধ্যে যোগাযোগের নতুন ধারা তৈরি করেছে। বড় রিটেইল আউটলেট ও ছোট ব্যবসায়ী উভয়ের জন্যই অনলাইনে কেনাকাটা বেড়েছে।

ইন্টারনেটে ব্যবসা-থেকে-ব্যবসা ও আর্থিক পরিষেবাগুলো সমগ্র শিল্পজুড়ে সরবরাহ চেইনকে প্রভাবিত করে। ইন্টারনেটের উৎপত্তি ১৯৬০-এর দশকে প্রাইভেট এবং ইউনাইটেড স্টেটস সামরিক গবেষণার মাধ্যমে একটি শক্তিশালী ও ত্রুটি-সহনশীল কম্পিউটার নেটওয়ার্কে পরিণত হয়েছে। ন্যাশনাল সায়েন্স ফাউন্ডেশনের দ্বারা একটি নতুন মার্কিন ব্যাকবোন তৈরির তহবিল, সেইসঙ্গে অন্যান্য বাণিজ্যিক ব্যাকবোনের জন্য ব্যক্তিগত তহবিল, নতুন নেটওয়ার্কিং প্রযুক্তির উন্নয়নে ও বিশ্বব্যাপী সবার অংশগ্রহণে সাহায্য করেছে। ১৯৯০-এর দশকের মাঝামাঝি সময়ে যা একটি আন্তর্জাতিক নেটওয়ার্ক ছিল তার বাণিজ্যিকীকরণের ফলে আধুনিক মানব জীবনের কার্যত প্রতিটি ক্ষেত্রে এর জনপ্রিয়তা এবং অন্তর্ভুক্তি ঘটে। এখন পৃথিবীর জনসংখ্যার আনুমানিক অর্ধেক ইন্টারনেট পরিষেবা ব্যবহার করছে।

প্রযুক্তিগত বাস্তবায়ন বা অ্যাক্সেস এবং ব্যবহারের জন্য ইন্টারনেটের কোনো কেন্দ্রীভূত নীতি নেই; প্রতিটি নেটওয়ার্ক তার নিজস্ব মান নিজেই সেট করে। কেবলমাত্র ইন্টারনেটের দুটি প্রধান বিষয়, ইন্টারনেট প্রোটোকল (IP) অ্যাড্রেস এবং ডোমেইন নেম সিস্টেম (DNS) এর নিয়ন্ত্রণ করা হয় একটি আন্তর্জাতিক সংস্থার মাধ্যমে যার নাম—'ইন্টারনেট কর্পোরেশন ফর অ্যাসাইনড নেমস অ্যান্ড নম্বরস' (ICANN) আর মূল প্রোটোকলের (IPV4 এবং IPV6) প্রযুক্তিগত স্টেন্ডার্ড নির্ধারন করে 'ইন্টারনেট ইঞ্জিনিয়ারিং টাস্ক ফোস'(IETF), যা একটি অলাভজনক সংস্থা, যার সঙ্গে যে কেউ প্রযুক্তিগত দক্ষতার অবদানের মাধ্যমে যুক্ত হতে পারে।

### ৮.২. ডাব্লিউডাব্লিউডাব্লিউ (www)

ওয়ার্ল্ড ওয়াইড ওয়েব, সংক্ষেপে ডাব্লুউডাব্লুউডাব্লুউ নামে পরিচিত এবং সাধারণত 'ওয়েব' নামে পরিচিত যাহা ইন্টারনেটের মাধ্যমে অ্যাক্সেস করা আন্তঃসংযুক্ত হাইপারটেক্সট নথিগুলোর একটি সিস্টেম। একটি ওয়েব ব্রাউজার দিয়ে, কেউ এমন ওয়েব পৃষ্ঠাগুলো দেখতে পারে যাতে পাঠ্য, ছবি, ভিডিও এবং অন্যান্য মাল্টিমিডিয়া থাকতে পারে এবং হাইপারলিঙ্ক ব্যবহার করে তাদের মধ্যে নেভিগেট করতে পারে। পূর্ববর্তী হাইপারটেক্সট সিস্টেমের ধারণাগুলো ব্যবহার করে, ইংরেজ প্রকৌশলী এবং কম্পিউটার বিজ্ঞানী স্যার টিম বার্নার্স-লি, বর্তমানে ওয়ার্ল্ড ওয়াইড ওয়েব কনসোর্টিয়ামের পরিচালক, ১৯৮৯ সালের মার্চ মাসে একটি প্রস্তাব লিখেছিলেন, যা অবশেষে ওয়ার্ল্ড ওয়াইড ওয়েবে পরিণত হয়। ওয়ার্ল্ড ওয়াইড ওয়েব (ডাব্লুউ৩) মানুষের জ্ঞান এবং মানবসংস্কৃতির একটি পুল হিসাবে তৈরি করা হয়েছিল, যা দূরবর্তী সাইটগুলোতে সহযোগীদের তাদের ধারণা এবং একটি সাধারণ প্রকল্পের সমস্ত দিক শেয়ার করার সুযোগ দেয়।

### ৮.৩. হাইপারটেক্সট (Hypertext)

হাইপারটেক্সট হলো একটি কম্পিউটার বা অন্যান্য ইলেকট্রনিক ডিভাইসে অন্যান্য পাঠ্যের রেফারেন্স (হাইপারলিঙ্ক) যা পাঠক একটি মাউস ক্লিক বা কয়েকটি কীপ্রেসের মাধ্যমে অবিলম্বে অ্যাক্সেস করতে পারে। চলমান পাঠ্য ছাড়াও, হাইপারটেক্সটে টেবিল, চিত্র এবং অন্যান্য উপস্থাপনামূলক ডিভাইস থাকতে পারে। হাইপারটেক্সট হলো একটি অন্তর্নিহিত ধারণা, যা ওয়ার্ল্ড ওয়াইড ওয়েবের কাঠামোকে নতুন করে সংজ্ঞায়িত করে, ফলে ইন্টারনেটে তথ্য শেয়ার করার জন্য সহজ ও নমনীয় বিন্যাস তৈরি হয়।

### ৮.৪. হাইপারলিঙ্ক (Hyperlink)

হাইপারলিঙ্ক হলো একটি নথির একটি রেফারেন্স, যা পাঠক সরাসরি অনুসরণ করতে পারে, বা এটি স্বয়ংক্রিয়ভাবে অনুসরণ করা যায়। রেফারেন্স একটি সম্পূর্ণ নথি বা একটি নথির মধ্যে একটি নির্দিষ্ট উপাদান নির্দেশ করে। হাইপারলিঙ্ক অনুসরণকারী ব্যবহারকারীকে হাইপারটেক্সট নেভিগেট বা ব্রাউজ (Browse) করতে বলা হয়।

### ৮.৫. ওয়েব ব্রাউজার (Web Browser)

একটি ওয়েব ব্রাউজার বা ইন্টারনেট ব্রাউজার হলো ওয়ার্ল্ড ওয়াইড ওয়েবে তথ্য সংস্থান পুনরুদ্ধার, উপস্থাপন এবং চলাচলের জন্য একটি সফ্টওয়্যার অ্যাপ্লিকেশন। যদিও ব্রাউজারগুলো প্রাথমিকভাবে ওয়ার্ল্ড ওয়াইড ওয়েব অ্যাক্সেস করার উদ্দেশ্যে তৈরি করা হয়, তবে সেগুলো ব্যক্তিগত নেটওয়ার্কে বা ফাইল সিস্টেমে ফাইলগুলোতে ওয়েব সার্ভার দ্বারা প্রদত্ত তথ্য অ্যাক্সেস করতেও ব্যবহার করা যেতে পারে।

### ৮.৬. ওয়েব পেজ (Web Page)

একটি ওয়েব Page বা ওয়েবপৃষ্ঠা হলো একটি নথি বা তথ্যের সংস্থান, যা ওয়ার্ল্ড ওয়াইড ওয়েবের জন্য উপযুক্ত এবং একটি ওয়েব ব্রাউজারের মাধ্যমে অ্যাক্সেস করা যায় এবং একটি মনিটর বা মোবাইল ডিভাইসে প্রদর্শিত হতে পারে। এই তথ্য সাধারণত এইচটিএমএল বা এক্সএইচটিএমএল ফরম্যাটে থাকে এবং হাইপারটেক্সট লিঙ্কের মাধ্যমে অন্যান্য ওয়েব পৃষ্ঠাগুলোতে নেভিগেশন প্রদান করতে পারে। ওয়েবপৃষ্ঠাগুলো স্থানীয় কম্পিউটার বা দূরবর্তী ওয়েব সার্ভার থেকে পুনরুদ্ধার করা যেতে পারে। ওয়েব সার্ভার শুধু একটি ব্যক্তিগত নেটওয়ার্কে যেমন একটি কর্পোরেট ইন্ট্রানেট (Intranet) অ্যাক্সেস সীমাবদ্ধ থাকতে পারে, অথবা, এটি ওয়ার্ল্ড ওয়াইড ওয়েবে পৃষ্ঠাগুলো প্রকাশ করতে পারে।

ওয়েবপেজগুলো ওয়েব সার্ভারের ফাইল সিস্টেমের মধ্যে সংরক্ষিত স্ট্যাটিক টেক্সট এবং অন্যান্য বিষয়বস্তু নিয়ে গঠিত হতে পারে (স্ট্যাটিক ওয়েবপেজ) অথবা অনুরোধ করা হলে সার্ভার-সাইড সফ্টওয়্যার দ্বারা নির্মিত হতে পারে (ডাইনামিক ওয়েবপেজ)।

### ৮.৭. ইন্টারনেট বনাম ডাব্লিউডাডিব্লউডাব্লিউ (Internet vs WWW)

ইন্টারনেট এবং ওয়ার্ল্ড ওয়াইড ওয়েব শব্দগুলো প্রায়শই দৈনন্দিন বক্তৃতায় খুব বেশি পার্থক্য ছাড়াই ব্যবহৃত হয়। যা হোক, ইন্টারনেট এবং ওয়ার্ল্ড ওয়াইড ওয়েব এক নয়। ইন্টারনেট একটি বিশ্বব্যাপী তথ্য যোগাযোগ ব্যবস্থা। এটি একটি হার্ডওয়্যার এবং সফ্টওয়্যার অবকাঠামো যা কম্পিউটারের মধ্যে সংযোগ প্রদান করে। বিপরীতে, ওয়েব হলো ইন্টারনেটের মাধ্যমে যোগাযোগ করা পরিষেবাগুলোর মধ্যে একটি। এটি হাইপারলিঙ্ক এবং ইউআরএল দ্বারা সংযুক্ত আন্তঃসংযুক্ত নথি এবং অন্য সংস্থানগুলোর একটি সংগ্রহ।

### ৮.৮. ইউআরএল (URL)

ইউনিফর্ম রিসোর্স লোকেটার (URL) হলো একটি ইউনিফর্ম রিসোর্স আইডেন্টিফায়ার (ইউআরআই) যা নির্দিষ্ট করে যে একটি নির্দিষ্ট রিসোর্স কোথায় পাওয়া যায় এবং এটি পুনরুদ্ধার করার পদ্ধতি কী? একটি URL এর সবচেয়ে পরিচিত উদাহরণ হলো ওয়ার্ল্ড ওয়াইড ওয়েবে একটি ওয়েব পৃষ্ঠার 'ঠিকানা', যেমন http://www.dutchbanglabank.com.

### ৮.৯. ই-মেইল (e-mail)

ইলেকট্রনিক মেল, যাকে সাধারণত ইমেল বা ই-মেইল বলা হয়, ইন্টারনেট বা অন্যান্য কম্পিউটার নেটওয়ার্কে ডিজিটাল বার্তা আদান-প্রদানের জন্য ব্যবহৃত একটি পদ্ধতি। মূলত, ইমেল সরাসরি একটি কম্পিউটার থেকে অন্য আরেকটি কম্পিউটারে প্রেরণ করা হয়। এর জন্য উভয় কম্পিউটারকে একই সময়ে অনলাইন থাকতে হত। কিন্তু আজকের ইমেল সিস্টেমগুলো একটি স্টোর-এবং-ফরোয়ার্ড মডেলের ওপর ভিত্তি করে। ইমেল সার্ভার বার্তা গ্রহণ করে, ফরোয়ার্ড করে, বিতরণ করে এবং সংরক্ষণ করে। ব্যবহারকারীদের আর একসঙ্গে অনলাইনে থাকতে হয় না এবং শুধু ক্ষণিক সময়ের জন্য সংযুক্ত হতে হয়, সাধারণত একটি ইমেল সার্ভারের যতক্ষণ বার্তা পাঠাতে বা গ্রহণ করতে সময় লাগে ততক্ষণ।

একটি ইমেল বার্তা দুটি উপাদান নিয়ে গঠিত, বার্তা শিরোনাম এবং বার্তার মূল অংশ, যা ইমেলের বিষয়বস্তু। বার্তা শিরোনামে নিয়ন্ত্রণ তথ্য রয়েছে, যার মধ্যে রয়েছে, কমপক্ষে, প্রেরকের ইমেল ঠিকানা, এক বা একাধিক প্রাপকের ঠিকানা, এবং একটি বিষয় বা শিরোনাম। ইমেল মাল্টি-মিডিয়া বিষয়বস্তু সংযুক্তি হিসাবে বহন করতে পারে।

# পর্যালোচনমূলক প্রশ্নাবলি

## 1 Multiple Choice Questions (MCQ)

i) Which computer was made of Vacuum tube?
a) IBM b) ENIAC c) NCR d) ABC

ii) Which computer was made of Valve?
a) IBM b) ENIAC c) NCR d) ABC

iii) What was the weight of ENIAC computer?
a) 3 tons b) 30 tons c) 3 kg d) 30 kg

iv) The first computer in Bangladesh
-was installed in which year of
a) 1971 b) 1961 c) 1964 d) 1984
- was installed by
a) BUET b) Bangladesh Atomic Energy Commission c) Bureau of Statistics d) Agrani Bank
- was a type of the computer
a) Super Computer b) Mainframe c) Micro Computer d) PC

v) Which of the following is not an application software?
a) MS Word b) Excel c) Windows d) Firefox

vi) Banking software is a/an
a) Operating System b) Database c) Application software d) Programming language.

vii) Which one is an Object Oriented Program Language?
a) Java b) Basic c) Fortran d) Cobol

viii) Internet uses a standard internet protocol suite called
a) www b) TCP/IP c) WAN d) Fiber Optic

ix) Which one is not an electronic banking system:
a) ATM b) Internet Banking c) POS terminal d) Cash
b) Counter

x) Which functionality is not available in an Internet Banking System?
a) Cash withdrawal b) Balance Check c) Fud transfer d) Pay
b) Utility Bills

xi) Which of the following is not an input device of a computer?
a) Keyboard b) Scanner c) RAM d) Microphone

xii) Which of the following is not an input device of a computer?
a) Monitor b) Speaker c) Printer d) Scanner

xiii) Which of the following is not a programming language?
a) Java b) C++ c) BASIC d) Excel

## 2 Fill in the gap

i) Microcomputer was developed in ------- using ----------.

ii) Operating systems were first developed in ----- for --------.

iii) Internet started in ---- as research work and become International Network in ------.

iv) ATM is used mainly for withdrawal of cash by a bank customer using his debit, credit or ----- card.

v) ATM is supplied with a device for reading a card and a ---- for interaction with the cardholder.

vi) MFS is a banking system for ------- populations.

vii) P2P stands for -------.

viii) MFS was started in Bangladesh in the year of --------.

ix) Buying and selling of goods and services over ------- is called e-commerce.

x) -------- is called the father of computer?

xi) First electronic computer produced commercially was developed in the year of ------.

xii) Bangladesh Atomic Energy Commission installed first computer in Bangladesh in the year of -------.

xiii) Three types of computer are: -------- computer, digital computer and ------- computer.

ix) Based on the size and capacity, computer can be divided into four types such as ------- computer, -------- computer, -------- computer and micro computer.

x) WWW stands for --------.

## সম্ভাব্য প্রশ্নাবলি

1. What is the difference between the terms 'Information Technology'and 'Information and Communication Technology'?
2. Define Information and Communication Technology (ICT).
3. Banking service is now available anytime. How ICT contributed to this?
4. Banking service is now available anywhere. How this become possible after implementation of ICT in Banking?
5. Narrate importance of use of ICT in Banking.
6. Name five electronic banking systems and define them.
7. What are the differences among ATM, CDM and CRM?
8. Name some components of an ATM and mention their functions.
9. How ATMs brings freedom to the customers?
10. Mention five functions of an ATM.
11. What is an ATM booth?
12. What kind of dispute may arise of a CDM? How banks mitigate this?
13. Describe steps of withdrawing money from ATM.
14. Describe various components of a POS terminal.
15. How GPRS POS terminal is different from a dial-up POS terminal?
16. How a bank earns from a POS terminal installed at a merchant?
17. Describe how payment is made using a POS terminal.

18. How Internet Banking works?
19. What banking activities a customer can perform using Internet Banking?
20. Can a customer receive cash from Internet Banking? Why?
21. Mention a few differences between sms and Alert Banking.
22. Mention two syntaxes for any two functions of sms banking.
23. Describe some advantages and disadvantages of Electronic Banking.
24. What is online banking or Any Branch banking? Mention advantages and disadvantages of online banking.
25. What is a MFS? Name a few remarkable MFS in Bangladesh.
26. When MFS started its journey in Bangladesh and which bank stated it?
27. What are the services a MFS operator provides in Bangladesh? Name 5 most used services which approximate amount of transactions through each of the services held in Feb, 2022.
28. As per the MFS policy, how much share a bank shall hold in the MFS?
29. In relation to e-commerce, define the following: Cart, Payment gateway, Acquiring and Issuing Bank, PIN, CVV, CVC, Payment Association, Authorization, Settlement, Nostro account, NPSB.
30. Describe process flow of payment in ecommerce.
31. Describe settlement process for ecommerce trasactions.
32. What is a computer? Who is the father of computer?
33. Describe different generation of computers.
34. Different types of computer are Analog, Digital and Hybrid. Describe each of them.
35. Based on size & capacity, computer can be divided into Super, Mainframe, Mini and Micro computers. What are the differences among them?
36. Why micro computers are also called as PC?
37. Name five input devices and 3 output devices. Describe printer, keyboard and mouse.
38. Differentiate between a dot matrix and a laser printer.
39. What stand for CPU? What is its use in computer?
40. What are CISC and RISC processor? Which processor is used in a high-end IBM server?
41. Narrate characteristics of each of the Main, Cache and Secondary memory.
42. What are differences among Floppy disk, Hard disk, CD and Pen drive?
43. What is a mother board?
44. Why an UPS is used with a computer?
45. What are the differences between a system software and application software?
46. What are the functionalities of an operating system?
47. Why a database is used along with a program?
48. Describe the following: a) DBA, b) Backup c) Database Management System
49. Define the followings: a) Internet, b) IP, c) DNS, d) Hyperlink, e) URL, f) email
50. Identify differences between IPv4 and IPv6?
51. What is World Wide Web? What is the basic difference between www and Internet?

মডিউল-বি

# আর্থিক প্রতিষ্ঠানের স্বয়ংক্রিয়করণের জন্য বিভিন্ন পদ্ধতি

## ১. ডেটা সেন্টার (ডিসি), নিয়ার ডিসি, ডিজাস্টার রিকভারি সাইট (ডিআরএস), ডেটা সেন্টার স্ট্যান্ডার্ড ও সার্টিফিকেশন

### ১.১. ডেটা সেন্টার (DC)

একটি ডেটা সেন্টার হলো একটি রেজ সিস্টেম, রাখার জন্য ব্যবহৃত হয়। এতে সাধারণত রিডান্ডেন্ট বা ব্যাকআপ পাওয়ার সাপ্লাই, রিডান্ডেন্ট ডেটা যোগাযোগ সংযোগ, পরিবেশগত নিয়ন্ত্রণ (যেমন, এয়ার কন্ডিশনার, অগ্নি দমন) ও নিরাপত্তা ডিভাইসসমূহ অন্তর্ভুক্ত থাকে।

*ডেটা সেন্টার*

বর্তমানে চার ধরনের ডেটা সেন্টার রয়েছে। সবচেয়ে সহজ হলো টিয়ার-১ ডেটা সেন্টার, যা মূলত একটি সার্ভার রুম, যা কম্পিউটার সিস্টেম ইনস্টল করার জন্য প্রাথমিক নির্দেশিকা অনুসরণ করা হয়। সবচেয়ে উন্নততম স্তর হলো টায়ার ৪ ডেটা সেন্টার, যা মিশন-ক্রিটিক্যাল কম্পিউটার সিস্টেমগুলোকে হোস্ট করার জন্য ডিজাইন করা হয়, যা সম্পূর্ণ রিডান্ডেন্ট সাবসিস্টেম এবং বায়োমেট্রিক অ্যাক্সেস কন্ট্রোল পদ্ধতি দ্বারা নিয়ন্ত্রিত কম্পার্টমেন্টালাইজড সিকিউরিটি জোন দ্বারা সজ্জিত। ডিসি এর ৪টি স্তরের প্রত্যেকটি নিচে বর্ণিত হয়েছে—

| টিয়ার লেভেল/স্তর | প্রয়োজনীয়তা |
|---|---|
| ১. | • একক নন-রিডান্ডেন্ট আইটি সরঞ্জাম সজ্জিত।<br>• নন-রিডান্ডেন্ট সক্ষমতা<br>• মৌলিক সাইট পরিকাঠামো যাহা ৯৯.৬৭১% প্রাপ্যতার গ্যারান্টি দেয়। |
| ২. | • সমস্ত স্তর ১ এর প্রয়োজনীয়তা পূরণ করে<br>• রিডান্ডেন্ট সক্ষমতা যা ৯৯.৭৪১% প্রাপ্যতার গ্যারান্টি দেয়। |
| ৩. | • সব টিয়ার ১ এবং টিয়ার ২ এর প্রয়োজনীয়তা পূরণ করে<br>• আইটি সরঞ্জাম পরিবেশন করা একাধিক স্বাধীন বণ্টন পাথ<br>• সমস্ত আইটি সরঞ্জাম অবশ্যই দ্বৈত-বিদ্যুৎ চালিত এবং সাইটের আর্কিটেকচারের টপোলজির সঙ্গে সম্পূর্ণ সামঞ্জস্যপূর্ণ হতে হবে<br>• একযোগে রক্ষণাবেক্ষণযোগ্য সাইট অবকাঠামো, যা ৯৯.৯৮২% প্রাপ্যতার গ্যারান্টি দেয়। |
| ৪. | • সমস্ত টিয়ার ১, টিয়ার ২ এবং টিয়ার ৩ এর প্রয়োজনীয়তা পূরণ করে<br>• সমস্ত কুলিং সিস্টেম স্বাধীনভাবে দ্বৈত-বিদ্যুৎ চালিত<br>• বৈদ্যুতিক পাওয়ার ও স্টোরেজসহ ত্রুটি-সহনশীল একটি অবকাঠামো, যা ৯৯.৯৯৯৯% প্রাপ্যতার গ্যারান্টি দেয়। |

একটি ডেটা সেন্টার একটি বিল্ডিংয়ের একটি কক্ষ, এক বা একাধিক ফ্লোর বা একটি সম্পূর্ণ বিল্ডিং দখল করতে পারে। বেশিরভাগ সরঞ্জামগুলো প্রায়ই রেক ক্যাবিনেটে মাউন্ট করা থাকে, যা সাধারণত তাদের মধ্যে করিডোর তৈরি করে একক সারিগুলোতে স্থাপন করা হয়। এটি প্রতিটি ক্যাবিনেটের সামনে এবং পিছনের দিকে লোকেদের যাতায়াতের সুবিধা দেয়। ডেটা সেন্টারে তাপমাত্রা ও আর্দ্রতা নিয়ন্ত্রণ করতে এয়ার কন্ডিশনার ব্যবহার করা হয়। সুপারিশকৃত তাপমাত্রা

১৬-২৪ ডিগ্রি সেলসিয়াস (৬৪-৭৫ ডিগ্রি ফারহেনহাইট) এবং আর্দ্রতার পরিমাণ ৪০-৫৫% এবং সর্বোচ্চ ডিউ পয়েন্ট ১৫ ডিগ্রি সেলসিয়াস।

### ১.২. নিয়ার ডিসি (Near D.C.)

নিয়ার ডেটা সেন্টার হলো একই শহরে প্রতিষ্ঠিত একটি ডেটা সেন্টার যেখানে প্রধান ডেটা সেন্টারটি অবস্থিত। প্রধান ডেটা সেন্টার এবং নিয়ার ডেটা সেন্টারকে কখনও কখনও যথাক্রমে ডিসি ১ এবং ডিসি ২ হিসাবে উল্লেখ করা হয়। ডিসি ১ এবং ডিসি ২ উভয়ই একই ধরনের হার্ডওয়্যার ও অন্যান্য ডিভাইস এবং সফ্টওয়্যারসহ ইনস্টল করা হয় এবং এক্টিভ-এক্টিভ মোডে সেট আপ করা হয়। উভয় ডেটা সেন্টারের সমস্ত রিসোর্স একই সঙ্গে ৫০-৫০ লোডে ব্যবহার করা হয়। যদি ডিসি ১ এবং ডিসি ২-এর মধ্যে একটি যে কোনো কারণে বন্ধ হয়ে যায়, অন্যটি কোনো বাধা ছাড়াই একা ব্যাংকের অপারেশন চালাতে পারে এবং এই অপারেশনের সুইচিং পদ্ধতিগুলো স্বয়ংক্রিয়ভাবে হয়ে থাকে—শাখা, এটিএম এবং অন্যান্য চ্যানেলের ব্যবহারকারীরা কিছুই বুঝতেই পারেন না। ডিসি ১ এবং ডিসি ২ আইটি লোকেদের জন্য তাদের আইটি অফিস থেকে ন্যূনতম ভ্রমণের সময়ে সহজে অ্যাক্সেসযোগ্য হওয়া উচিত। আইটি অফিস হল ডিসি ১ এবং ডিসি ২ ব্যতীত অন্য একটি অফিস যেখানে আইটি বিশেষজ্ঞরা বসে সমস্ত আইটি-সম্পর্কিত কার্যক্রম সম্পাদন করেন।

### ১.৩. ডিজাস্টার রিকভারি সাইট (DRS)

ডিজাস্টার রিকভারি হল প্রাকৃতিক বা মানব-প্ররোচিত দুর্যোগের পরে একটি সংস্থা কীভাবে তার কার্যাবলি অব্যাহত রাখবে তার জন্য প্রস্তুত করা বিভিন্ন প্রক্রিয়া, নীতি এবং পদ্ধতি। একটি ডিজাস্টার রিকভারি সাইট হলো ডেটা সেন্টারের মতোন একটি স্থান যেখানে একই ধরনের অবকাঠামো, হার্ডওয়্যার এবং সফ্টওয়্যার ইনস্টল করা এবং ডেটা সংরক্ষণ করা হয়। ডেটা সেন্টার বিপর্যয়ের ক্ষেত্রে স্বয়ংক্রিয়ভাবে তাহা প্রাথমিক সাইট হয়ে ওঠার ক্ষমতা থাকা উচিত।

ডেটা সেন্টার ও ডিআরএসের মধ্যে দূরত্ব নিম্নলিখিত দুটি সমস্যার মধ্যে ট্রেড-অফ করতে হবে—

১. যদি একটি দীর্ঘ দূরত্ব বেছে নেওয়া হয়, তাহলে DRS-এর ব্যবস্থাপনা, ডার্ক ফাইবারের প্রাপ্যতা এবং প্রয়োজনীয় লেটেন্সির প্রাপ্যতা সম্পর্কিত সমস্যা হতে পারে। এছাড়াও, Sync replication তৈরি সম্ভব নাও হতে পারে।

২. যদি একটি স্বল্প দূরত্ব (অন্তত ২০ কিমি) বেছে নেওয়া হয়, তবে ভূমিকম্প বা হারিকেনের মতো একটি বিপর্যয় উভয় সাইটকে ধ্বংস করে দিতে পারে।

৩. DC এবং DRS দুটি ভিন্ন সিস্মিক জোনে (Zone) স্থাপন করতে হবে।

### ১.৪. ডেটা সেন্টার স্ট্যান্ডার্ড ও সার্টিফিকেশন

ডেটা সেন্টার সার্টিফিকেশন ও স্ট্যান্ডার্ড একটি ডেটা সেন্টারের অপারেশনাল নিরাপত্তা ও অপারেশনের ধারাবাহিকতা নিশ্চিত করে। এটি উচ্চ নির্ভরযোগ্যতা এবং কর্মক্ষমতা নিশ্চিত করে, যা একটি সাধারণ কোম্পানির সার্ভার রুমে অর্জন করা কঠিন হতে পারে। 'আপটাইম ইনস্টিটিউট' দ্বারা প্রদত্ত ডেটা সেন্টার সার্টিফিকেশনগুলোর মধ্যে একটি হলো টিয়ার সার্টিফিকেশন (টায়ার-১, টায়ার-২, টায়ার-৩, বা টায়ার-৪)।

অন্যদিকে ডেটা সেন্টার স্ট্যান্ডার্ড, ডেটা সেন্টারের উচ্চতর সুরক্ষা নিশ্চিত করে। সবচেয়ে বেশি ব্যবহৃত স্ট্যান্ডার্ড হলো আইএসও ২৭০০০, পিসিআই ডিএসএস, এইচআইপিএএ, টিআইএ ৯৪২ বা এআইসিপিএ এসওসি। মডিউল ডি-তে ডেটা সেন্টারের নিরাপত্তা নিয়ে বিস্তারিত আলোচনা করা হবে।

### ডেটা সেন্টারের স্তর

- টায়ার-১ : এই ডেটা সেন্টারগুলো সবচেয়ে সাশ্রয়ী মূল্যের হোস্টিং পরিবেশ নিশ্চিত করে এবং সেটি ছোট ব্যবসা ও স্টার্ট-আপগুলোর জন্য সবচেয়ে উপযুক্ত। জটিল আইটি অবকাঠামো ছাড়া ছোট সংস্থাগুলো যেগুলো ঘন ঘন ডাউনটাইম সহ্য করতে পারে, তারা টিয়ার-১ মান গ্রহণের জন্য উপযুক্ত। টায়ার-১ ডেটা সেন্টারে পাওয়ার এবং কুলিং এর জন্য একটি মাত্র ব্যবস্থা রয়েছে এবং কোনো ব্যাকআপ এর সুবিধা নেই। এই স্তরটির ৯৯.৬৭১% প্রত্যাশিত আপটাইম প্রদান করে।
- টিয়ার-২ : এই ডেটা সেন্টারগুলো হলো এসএমই ব্যবসার জন্য উপযুক্ত, যারা টিয়ার-১ স্ট্যান্ডার্ডের চেয়ে সাশ্রয়ী, আরও নির্ভরযোগ্য ব্যবস্থা চায়। ছোট থেকে মাঝারি আকারের সংস্থাগুলো সাধারণত নন-মিশন-ক্রিটিক্যাল ডেটাবেস হোস্ট করতে টিয়ার-২ ডেটা সেন্টার ব্যবহার করে। টায়ার-২ ডেটা সেন্টারে পাওয়ার এবং কুলিংয়ের জন্য একটি মাত্র ব্যবস্থা রয়েছে এবং আইটি সরঞ্জামের জন্য কিছু রিডান্ডেন্ট এবং ব্যাকআপ সুবিধা রয়েছে। এই স্তরটি ৯৯.৭৪১% এর প্রত্যাশিত আপটাইম নিশ্চিত করে।
- টায়ার-৩ : এই ধরনের ডেটা সেন্টার বড় কোম্পানিগুলোর আইটি অপারেশনের জন্য আদর্শ, যেখানে অতিরিক্ত নিরাপত্তা প্রয়োজন। বিস্তৃত ডেটা নিয়ে কাজ করে এমন ব্যবসাগুলো (বিশেষত গ্রাহক ডেটা) এই স্তরের জন্য প্রধান প্রার্থী। টায়ার ৩ ডেটা সেন্টারে পাওয়ার এবং কুলিংয়ের জন্য একাধিক পাথ এবং রিডান্ডেন্ট সিস্টেম রয়েছে, যা কর্মীদের অফলাইনে না নিয়ে

অবিরাম কাজ করার সুযোগ দেয়। এই স্তরে ৯৯.৯৮২% প্রত্যাশিত আপটাইম নিশ্চিত করে।

- টায়ার-৪ : এই ডেটা সেন্টারগুলো, নিরবচ্ছিন্ন প্রাপ্যতা প্রয়োজন এবং বাজেটের সীমাবদ্ধতা নেই এমন এন্টারপ্রাইজগুলোর জন্য উপযুক্ত। সরকারি সংস্থা, ব্যাংক ও বড় সংস্থা যাদের মিশন-ক্রিটিক্যাল সার্ভার এবং ব্যবসার চাহিদা রয়েছে তাদের স্তর-৪ সুবিধার ডেটা সেন্টারের প্রয়োজন। টায়ার-৪ ডেটা সেন্টার একটি সম্পূর্ণ ত্রুটি-সহনশীল ডেটা সেন্টার। এই স্তরটি ৯৯.৯৯৫% এর প্রত্যাশিত আপটাইম নিশ্চিত করে।

  সাধারণত, একটি স্তর নির্বাচন করার সময় দুটি প্রাথমিক বিবেচ্য হলো মূল্য এবং আপটাইম।

## ২. কম্পিউটার নেটওয়ার্কিং

### ২.১. ল্যান ও ওয়্যানের ধারণা

#### ২.১.১. লোকাল এরিয়া নেটওয়ার্ক বা LAN

একটি লোকাল এরিয়া নেটওয়ার্ক (ল্যান) হলো একটি কম্পিউটার নেটওয়ার্ক যা একটি ছোট এলাকাকে কভার করে, যেমন একটি শাখা, বাড়ি, অফিস, বা বিল্ডিংয়ের ছোট গ্রুপ, যেমন একটি স্কুল বা বিমানবন্দর। LAN একাধিক কম্পিউটারকে সংযুক্ত করে এবং ফাইল, প্রিন্টার, গেম বা অন্যান্য অ্যাপ্লিকেশনের মতো রিসোর্সগুলো পরস্পরের সঙ্গে শেয়ার করতে পারে। একটি ল্যানের সঙ্গে

*নেটওয়ার্ক ক্যাবল*

সংযুক্ত একটি কম্পিউটার একই ল্যানের অন্য কম্পিউটারের সঙ্গে ডেটা ও প্রোগ্রামগুলো শেয়ার করতে সক্ষম। ব্যবহারকারীরা ই-মেইল পাঠিয়ে বা চ্যাট সেশনে জড়িত থাকার মাধ্যমে একে অপরের সঙ্গে যোগাযোগ করতে পারেন।

প্রতিটি কম্পিউটারে একটি ল্যান কার্ড ইনস্টল করা আছে। ল্যান কার্ডের একটি পোর্ট রয়েছে যেখানে একটি তারের এক প্রান্ত সংযুক্ত থাকে। তারের আরেকটি প্রান্ত একটি হাব বা নেটওয়ার্ক সুইচের সঙ্গে সংযুক্ত। একইভাবে, ল্যান তৈরি করার জন্য সমস্ত কম্পিউটার হাব বা নেটওয়ার্ক সুইচের সঙ্গে সংযুক্ত থাকে। প্রতিটি ইথারনেট তারের দৈর্ঘ্য প্রায় ১০০ মিটারের মধ্যে থাকতে হয়। নিম্নলিখিত বৈশিষ্ট্যগুলো একটি ল্যানকে অন্যটি থেকে আলাদা করে—

**টপোলজি** : ইহা নেটওয়ার্কে ডিভাইসের জ্যামিতিক বিন্যাস নির্দেশ করে। উদাহরণস্বরূপ, ডিভাইসগুলো একটি রিং বা একটি সরল রেখায় সাজানো যেতে পারে।

**প্রোটোকল** : ইহা ডেটা পাঠানোর নিয়ম এবং এনকোডিং স্পেসিফিকেশন নির্ধারন করে। প্রোটোকলগুলো নির্ধারণ করে যে নেটওয়ার্কটি পিয়ার-টুপিয়ার না ক্লায়েন্ট/সার্ভার আর্কিটেকচার ব্যবহার করবে।

**মিডিয়া** : ডিভাইসগুলো টুস্টেড-পেয়ার ওয়্যার, কোএক্সিয়াল ক্যাবল বা ফাইবার অপটিক ক্যাবল দ্বারা সংযুক্ত হতে পারে। কিছু নেটওয়ার্ক মিডিয়াকে ব্যবহার না করে রেডিওর মাধ্যমে যোগাযোগ করে।

ল্যানগুলো খুব দ্রুত হারে ডেটা প্রেরণ করতে সক্ষম, টেলিফোন লাইনের মাধ্যমে ডেটা প্রেরণের চেয়ে অনেক দ্রুত; কিন্তু দূরত্বেও সীমাবদ্ধতা রয়েছে, তাছাড়া একটি একক ল্যানের সঙ্গে কতটি কম্পিউটার সংযুক্ত করা যেতে পারে তারও সীমাবদ্ধতা রয়েছে।

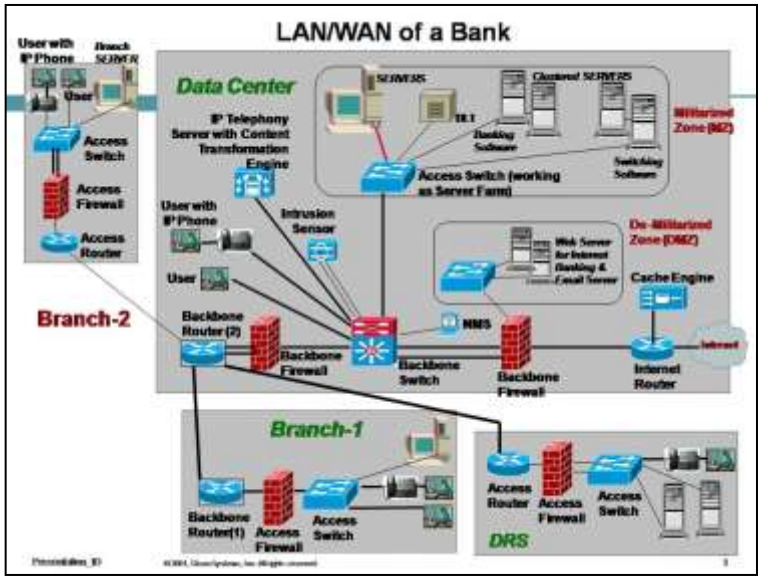
ওয়াইড এরিয়া নেটওয়ার্ক (ওয়্যান) এর বিপরীতে ল্যান-এর বৈশিষ্ট্যগুলোর মধ্যে রয়েছে তাদের উচ্চতর ডেটা-ট্রান্সফার রেট, ছোট ভৌগোলিক এলাকা এবং টেলিকমিউনিকেশন লাইনের অপ্রয়োজনীয়তা।

#### ২.১.২. ওয়াইড এরিয়া নেটওয়ার্ক বা WAN

ওয়াইড এরিয়া নেটওয়ার্ক (ওয়্যান) হলো একটি কম্পিউটার নেটওয়ার্ক যা একটি অপেক্ষাকৃত বড় ভৌগোলিক এলাকা জুড়ে বিস্তৃত। সাধারণত, একটি ওয়্যান দুই বা ততোধিক লোকাল এরিয়া নেটওয়ার্ক (ল্যান) কে সংযুক্ত করে।

একটি ওয়াইড-এরিয়া নেটওয়ার্কের সঙ্গে সংযুক্ত কম্পিউটারগুলো প্রায়ই পাবলিক নেটওয়ার্কের মাধ্যমে সংযুক্ত থাকে, যেমন টেলিফোন সিস্টেম (এক্স.২৫ এবং ডিডিএন)। তারা লিজড লাইন (রেডিও, ফাইবার অপটিক, ইত্যাদি) বা

স্যাটেলাইট (ভিএসএটি) এর মাধ্যমেও সংযুক্ত হতে পারে। একটি ল্যানের সমস্ত কম্পিউটার একটি নেটওয়ার্ক সুইচের সঙ্গে সংযুক্ত থাকে। নেটওয়ার্ক সুইচ একটি রাউটারের (Router) সঙ্গে সংযোগ রয়েছে, যা হলো ল্যানের গেটওয়ে। ওয়্যান-




এ অংশগ্রহণকারী বিভিন্ন ল্যান-এর সমস্ত রাউটার তারপর টেলিফোন সিস্টেম, লিজড লাইন বা স্যাটেলাইট ব্যবহার করে একসঙ্গে সংযুক্ত করা হয়। টিসিপি/আইপি, এক্স.২৫, এটিএম, এবং ফ্রেম রিলের মতো নেটওয়ার্ক প্রোটোকলগুলো ট্রান্সপোর্ট ও অ্যাড্রেসিং ফাংশন প্রদান করতে ব্যবহৃত হয়— অর্থাৎ, ওয়্যান-এ একটি কম্পিউটারের অবস্থান এবং ডেটা/তথ্য এবং/অথবা যোগাযোগ স্থানান্তর করার জন্য একটি রুট নির্ধারণের জন্য ব্যবহৃত হয়।

একটি ব্যাংকের জন্য, প্রতিটি শাখার একটি ল্যান আছে। শাখার সমস্ত কম্পিউটার এক বা একাধিক নেটওয়ার্ক সুইচের সঙ্গে সংযুক্ত। নেটওয়ার্ক সুইচ একটি রাউটারের সঙ্গে সংযুক্ত। যদি একটি ব্যাংকের ১০০টি শাখা থাকে, তবে প্রতিটি পৃথক শাখায় ১০০টি রাউটার (Router) ইনস্টল করা আছে। এখন সমস্ত রাউটার একত্রে সংযুক্ত হয়ে একটি ওয়্যান গঠন করে। সমস্ত রাউটার ফাইবার অপটিক লিজড লাইন, রেডিও লিঙ্ক বা স্যাটেলাইট (VSAT) ব্যবহার করে সংযুক্ত থাকে। তারা সম্মিলিতভাবে 'যোগাযোগ মাধ্যম' (Communication Media) হিসাবে পরিচিত। বর্তমানে বৃহত্তম ওয়্যান হলো ইন্টারনেট।

ওয়্যান ব্যবহার করে, একজন ব্যবহারকারী এবং একটি কম্পিউটার অন্য অবস্থানের একজন ব্যবহারকারী এবং একটি কম্পিউটারের সঙ্গে যোগাযোগ করতে পারে। অনেক ওয়্যান একটি নির্দিষ্ট সংস্থার জন্য নির্মিত ও সেটি ব্যক্তিগত। অন্য ওয়্যানগুলো ইন্টারনেট পরিষেবা প্রদানকারীদের দ্বারা নির্মিত এবং একটি সংস্থার ল্যান থেকে ইন্টারনেটে সংযোগ প্রদানের জন্য ব্যবহার করা হয়।

### ২.১.৩. ট্রান্সমিশন মিডিয়া (Transmission Media)

ট্রান্সমিশন বা কমিউনিকেশন মিডিয়া হলো ল্যান ও ওয়্যান-এর সঙ্গে কম্পিউটারের সংযোগের জন্য ব্যবহৃত ফিজিক্যাল মিডিয়া।

#### ২.১.৩.১. ল্যানের জন্য ট্রান্সমিশন মিডিয়া

ল্যান-এর জন্য বিভিন্ন ধরনের ট্রান্সমিশন মিডিয়া রয়েছে, সবচেয়ে জনপ্রিয় হলো টুইস্টেড পেয়ার ওয়্যার (সাধারণ বৈদ্যুতিক তার), কোক্সিয়াল ক্যাবল (কেবল টেলিভিশন এর জন্য ব্যবহৃত তার), ফাইবার অপটিক ক্যাবল (কাচ থেকে তৈরি তার), এবং তারহীন মাধ্যম (ওয়াই-ফাই)।

একটি ওয়াই-ফাই-সক্ষম ডিভাইস যেমন একটি কম্পিউটার, মোবাইল ফোন, বা MP3 প্লেয়ার, ইন্টারনেটের সঙ্গে সংযুক্ত একটি বেতার নেটওয়ার্কের সীমার মধ্যে থাকাকালীন ইন্টারনেটের সঙ্গে সংযোগ করতে পারে। ওয়াই-ফাই হটস্পট নামে পরিচিত বেতার নেটওয়ার্কের কভারেজ, একটি কক্ষ, একটি হোটেল, একটি বিশ্ববিদ্যালয় বা বিমানবন্দরের মতো ছোট এলাকা নিয়ে গঠিত হতে পারে। ওয়াই-ফাই হটস্পটগুলো সাধারণ জনগণকে বিনামূল্যে বা বিভিন্ন বাণিজ্যিক পরিষেবার গ্রাহকদের সাবস্ক্রিপশন ভিত্তিতে অ্যাক্সেস প্রদান করতে পারে।

#### ২.১.৩.২. ওয়্যান এর জন্য ট্রান্সমিশন মিডিয়া

ওয়্যান-এর জন্য ট্রান্সমিশন মিডিয়া হতে পারে একটি ল্যান্ড টেলিফোন সিস্টেম (এক্স.২৫, ডিডিএন, আইএসডিএন), লিজড ল্যান্ড লাইন (ফাইবার অপটিক), মাইক্রোওয়েভ (Radiolink), অথবা স্যাটেলাইট (VSAT)।

#### ক. ল্যান্ড লাইন (Land Line)

ল্যান্ড টেলিফোন সিস্টেম দুটি রাউটারের মধ্যে সরাসরি তামার তার ব্যবহার করে। এগুলো ধীরগতির (২ এমবি পর্যন্ত কম ব্যান্ডউইথ) এবং সারা দেশে পাওয়া যায় না। ফাইবার অপটিকের খুব উচ্চ ব্যান্ডউইথ রয়েছে (পরিষেবা প্রদানকারীরা ইন্টারফেস কার্ডের ওপর নির্ভর করে ১০ গিগাবাইট পর্যন্ত স্পিড পেতে পারে)। তবে এটি শুধু বড় শহরগুলোতে পাওয়া যায়।

**খ. মাইক্রোওয়েভ (Microwave)**

মাইক্রোওয়েভ বা রেডিও লিঙ্ক পাবলিক ফ্রিকোয়েন্সি (২.৪, ৫.৭ এবং ৫.৮ গিগাহার্টজ) এর পাশাপাশি লাইসেন্সকৃত ফ্রিকোয়েন্সি এর (৩.২ এবং ৫.২ গিগাহার্টজ) মাইক্রোওয়েভ ব্যবহার করে। দুটি পয়েন্ট একটি উচ্চ টাওয়ার এবং একটি অ্যান্টেনা ব্যবহার করে সংযুক্ত করা হয়। দুটি ল্যান সংযোগকারী দুটি অ্যান্টেনা অবশ্যই আই-টু-আই সংযুক্ত হতে হবে, অর্থাৎ, দুটি অ্যান্টেনার মধ্যে একটি বিল্ডিং বা পাহাড়ের মতো কোনো বাধা থাকা উচিত নয়। দুটি অ্যান্টেনার মধ্যে দূরত্ব ৩০ কিলোমিটারের বেশি হওয়া যাবে না। ইন্টারফেস কার্ডের ওপর নির্ভর করে ব্যান্ডউইথ সর্বাধিক ১০ এমবি হতে পারে (অর্থাৎ যদি ইন্টারফেস কার্ডের গতি ১০ এমবি হয়)।

মোবাইল ফোন সিস্টেম ডেটা সংযোগের জন্য বেতার প্রযুক্তি ব্যবহার করে। এই সিস্টেমগুলো কম ব্যান্ডউইথ (গতি) প্রদান করে এবং ব্যাংকের ডেটা সেন্টারের সঙ্গে অটোমেটেড টেলার মেশিন (এটিএম) সংযোগের জন্য ব্যবহার করা যেতে পারে।

**গ. স্যাটেলাইট (Sattelite)**

স্যাটেলাইট (VSAT= Very Small Aperture Terminal) দীর্ঘ দূরত্ব কভার করতে পারে। ভিসেট ব্যবহারের ক্ষেত্রে, এর অ্যান্টেনার জন্য আই-টু-আই সংযোগের কোনো প্রয়োজন নেই। যাহোক, ভিসেট একটি ছোট ব্যান্ডউইথ (১ এমবি পর্যন্ত) প্রদান করে, যা ব্যাংকিং অ্যাপ্লিকেশন চালানোর জন্য যথেষ্ট নাও হতে পারে। তবে তা এটিএম-এর সংযোগের জন্য ব্যবহার করা যেতে পারে।

**২.১.৪ ব্যাংকের জন্য ল্যান/ওয়্যান**

একটি ল্যান/ওয়্যান সেট আপ করার জন্য, আমাদের একটি হাব/নেটওয়ার্ক সুইচ ও রাউটার প্রয়োজন। যাইহোক, একটি ব্যাংকের জন্য, যা অর্থ নিয়ে কাজ করে এবং যেখানে নিরাপত্তাই প্রধান উদ্বেগের বিষয়, ডেটা সেন্টার, ডিআরএস এবং প্রতিটি শাখায় ফায়ারওয়ালের মতো অতিরিক্ত নিরাপত্তা ডিভাইসের প্রয়োজন হয়।

সুইচ এবং রাউটারের মধ্যে ফায়ারওয়াল ইনস্টল করা হয়। ফায়ারওয়াল গ্যারান্টি দেয় যে ডেটা সেন্টারে শুধু নির্ধারিত শাখা থেকেই নির্দেশাবলি আসছে।

**২.১.৪.১. ফায়ারওয়াল (Firewall)**

একটি ফায়ারওয়াল হলো একটি কম্পিউটার সিস্টেম বা নেটওয়ার্কের একটি অংশ যা শুধু অনুমোদিত স্থান/শাখা থেকেই নেটওয়ার্কে প্রবেশের অনুমতি দেয় এবং অন্য সব যোগাযোগ আটকিয়ে দেয়। এটি এমন একটি ডিভাইস যা নিয়ম এবং অন্যান্য মানদণ্ডের একটি সেটের ওপর ভিত্তি করে কম্পিউটার অ্যাপ্লিকেশনের অনুমতি বা অস্বীকার করার জন্য কনফিগার করা হয়েছে। ফায়ারওয়ালগুলো হার্ডওয়্যার বা সফ্টওয়্যার বা উভয়ের সংমিশ্রণে তৈরি করা যেতে পারে। অননুমোদিত ইন্টারনেট ব্যবহারকারীদের ইন্টারনেটের সঙ্গে সংযুক্ত ব্যক্তিগত নেটওয়ার্কগুলোতে অ্যাক্সেস করা থেকে বিরত রাখতে ফায়ারওয়ালগুলো প্রায়শই ব্যবহৃত হয়।

**২.১.৪.২. ডিএমজেড (DMZ)**

ডেটা সেন্টারে ইন্টারনেট সংযোগ দেওয়ার সময় বিশেষ নিরাপত্তার দিকে নজর দেওয়া প্রয়োজন। ইন্টারনেট অ্যাক্সেস সম্পর্কিত সার্ভারগুলোকে ডিমিলিটারাইজড জোনে (DMZ) স্থাপন করতে হয়।

কম্পিউটার নিরাপত্তায়, একটি ডিএমজেড বা ডিমিলিটারাইজড এলাকা হল একটি ভৌত বা লজিক্যাল সাব-নেটওয়ার্ক যা একটি প্রতিষ্ঠানের বাহ্যিক পরিষেবাগুলোকে একটি বৃহত্তর অবিশ্বস্ত নেটওয়ার্ক, সাধারণত ইন্টারনেটে উপস্থাপন করে। একটি ডিএমজেড এর উদ্দেশ্য হল একটি প্রতিষ্ঠানের ল্যান-এ নিরাপত্তার একটি অতিরিক্ত স্তর যোগ করা যাতে; একটি বহিরাগত আক্রমণকারীর, নেটওয়ার্কের অন্য কোনো অংশের পরিবর্তে শুধু ডিএমজেড-এ অবস্থিত সরঞ্জামগুলোতে অ্যাক্সেস করতে পারে।

**৩. আইটি সিস্টেম, স্টোরেজ ও ডাটাবেস ব্যাকআপ সিস্টেম**

ব্যাংক অটোমেশনের জন্য প্রচুর পরিমাণে হার্ডওয়্যার, স্টোরেজ ও সফ্টওয়্যার প্রয়োজন। সার্ভার, পার্সোনাল কম্পিউটার, ইউপিএস, বিভিন্ন সফটওয়্যার, নেটওয়ার্কিং ইকুইপমেন্ট এবং অন্যান্য আনুষঙ্গিকের জন্য বড় বিনিয়োগ প্রয়োজন। ৫০টি শাখার একটি ব্যাংকের অটোমেশনের জন্য প্রয়োজনীয় বাজেট প্রায় ৫০০-১০০০ মিলিয়ন টাকা হতে হবে। এই বাজেটে শুধু ডেটা সেন্টারের সেটআপ, ডিআরএস এবং সমস্ত শাখাকে একটি কোর ব্যাংকিং সলিউশনের মাধ্যমে অনলাইনে চালু করার জন্য প্রয়োজনীয় ইকুইপমেন্ট অন্তর্ভুক্ত করা হয়েছে এবং কোনও ডেলিভারি চ্যানেলের ইনস্টলেশন অন্তর্ভুক্ত নয়।

**৩.১. আইটি সিস্টেম ও স্টোরেজ**

আইটি সিস্টেমের মধ্যে রয়েছে স্টোরেজ সিস্টেম ব্যতীত সার্ভার, পার্সোনাল কম্পিউটার, ল্যাপটপ, প্রিন্টার, ইউপিএস, ভোল্টেজ স্টেবিলাইজার, জেনারেটর, ইত্যাদি। স্টোরেজ সিস্টেমের মধ্যে রয়েছে এক্সটার্নাল স্টোরেজ, স্যান সুইচ

ইত্যাদি। নিচে বিভিন্ন ধরনের সার্ভার ও সার্ভার ইনস্টলেশন সম্পর্কিত প্রযুক্তি (রেইড, ক্লাস্টারিং ও প্রতিলিপি) এবং এক্সটার্নাল স্টোরেজ ও স্যান সুইচ নিয়ে আলোচনা করা হলো।

### ৩.১.১. কম্পিউটার সার্ভার এবং প্রকারভেদ

কম্পিউটার সার্ভারগুলো শাখা ও ডেটা সেন্টারগুলোতে ব্যবহৃত হয়, যা একটি শাখায় অন্যান্য কম্পিউটার, সফ্টওয়্যার সিস্টেম বা ডাটাবেস পরিচালনা করে। বিভিন্ন ধরনের সার্ভার নিচে বর্ণনা করা হয়েছে—

#### ক. শাখা সার্ভার

একটি সার্ভার যা একটি শাখায় বসানো হয় এবং ল্যান-এর মাধ্যমে শাখার সমস্ত ব্যবহারকারীর (ব্যাংক অফিসারের) কম্পিউটার এর সঙ্গে সংযুক্ত থাকে। বিভিন্ন উদ্দেশ্যে এক বা একাধিক সার্ভার ল্যান এর সঙ্গে সংযুক্ত থাকতে পারে। ডেটা সেন্টারে কেন্দ্রীয়ভাবে ইনস্টল করা ব্যাংকের কোর ব্যাংকিং সিস্টেম অ্যাক্সেস করার জন্য এই ধরনের একটি সার্ভার ব্যবহার করা যেতে পারে। এটিকে শাখা সার্ভার বলা হয়। শাখা সার্ভার ব্যবহারকারীদের অনলাইন রিয়েল-টাইম ভিত্তিতে লেনদেন সম্পাদনের জন্য কেন্দ্রীয় অ্যাপ্লিকেশন সার্ভারগুলোতে অ্যাক্সেস করতে সহায়তা করে।

কোর ব্যাংকিং সফ্টওয়্যারের আগের সংস্করণগুলো ৪টি ধাপে কাজ করার জন্য ডিজাইন করা হয়েছিল—ব্যবহারকারী টার্মিনাল, শাখা সার্ভার, অ্যাপ্লিকেশন সার্ভার এবং ডাটাবেস সার্ভারে। শাখা সার্ভারটি অফলাইনে কিছু ক্রিয়াকলাপ সম্পাদন করতে এবং শাখা সার্ভার থেকে স্থানীয়ভাবে কিছু কার্যকারিতা যাচাই করতে ব্যবহৃত হয়েছিল, যা ফলস্বরূপ ওয়্যানের মাধ্যমে কেন্দ্রীয় সার্ভারে সংযোগের ক্ষেত্রে ব্যান্ডউইথের প্রয়োজনীয়তা হ্রাস করে। অফলাইন ক্ষমতা নিশ্চিত করে যে ওয়্যান সংযোগ বিচ্ছিন্ন হওয়ার পর, শাখা ব্যবহারকারীরা শুধু তাদের নিজস্ব (প্রধান ব্রাঞ্চ বা শাখা) গ্রাহকদের জন্য অফলাইন লেনদেন করতে পারেন। এই ধরনের অফলাইন লেনদেন ব্রাঞ্চ সার্ভারের ডাটাবেসে যাচাই করা ও রেকর্ড করা হয়। সংযোগ স্থাপনের পর, সমস্ত লেনদেন আপডেটের জন্য কেন্দ্রীয় ডাটাবেস সার্ভারে পাঠানো হয়। ব্রাঞ্চ সার্ভার হোম ব্রাঞ্চের গ্রাহকদের স্বাক্ষর এবং ফটোগ্রাফ রেকর্ড করে এবং হোম ব্রাঞ্চ থেকে লেনদেনের সময়, এগুলো যাচাইয়ের জন্য ব্রাঞ্চ সার্ভার থেকে ব্যবহারকারীর টার্মিনালে প্রদর্শিত হয়। এটি ব্যান্ডউইথের প্রয়োজনীয়তা হ্রাস করে। স্বাক্ষর এবং ছবি একই সঙ্গে ডেটা সেন্টারের কেন্দ্রীয় ডাটাবেস সার্ভারে রেকর্ড করা হয়। যদি একজন গ্রাহক অন্য শাখা থেকে লেনদেন করেন, তবে সেগুলো ডেটা সেন্টার থেকে ব্যবহারকারীর কম্পিউটারে প্রদর্শিত হয়।

যেহেতু ব্যান্ডউইথ প্রাপ্ততা সহজ এবং কম ব্যয়বহুল হয়ে উঠেছে, এই ব্যাংকগুলো এখন ডেটা সেন্টার এবং শাখাগুলোর মধ্যে একাধিক লিঙ্ক ব্যবহার করছে। ফলে এই ধরনের সফটওয়্যারের ব্যবহার ও শাখা সার্ভার স্থাপন এখন অপ্রয়োজনীয় হয়ে উঠেছে।

#### খ. অ্যাপ্লিকেশন সার্ভার

যখন একজন ব্যাংক অফিসার (ব্যবহারকারী) তার কম্পিউটার টার্মিনালে একটি পোস্টিং করেন, প্রথমে এটি শাখা সার্ভারে আংশিকভাবে যাচাই করা হয়। তারপর ডেটা এবং নির্দেশাবলি ওয়্যান-এর মাধ্যমে ডেটা সেন্টারের অ্যাপ্লিকেশন সার্ভারে চলে যায়। অ্যাপ্লিকেশন সার্ভার হলো একটি সার্ভার, যা নির্দিষ্ট উদ্দেশ্যে লেখা প্রোগ্রামের প্রধান অংশসমূহ ধারণ করে। প্রোগ্রামিং কৌশলের ৩-স্তরের আর্কিটেকচারে, সাধারণত ব্যবহারকারীর কম্পিউটার বা টার্মিনাল, অ্যাপ্লিকেশন সার্ভার এবং ডাটাবেস সার্ভার জড়িত থাকে। প্রোগ্রামটির একটি অংশ ব্যবহারকারীর কম্পিউটার বা টার্মিনালে ইনস্টল করা হয়। ব্যবহারকারীকে একটি আইকন বা মেনুতে ক্লিক করে এই প্রোগ্রামটি চালাতে হয়। এই প্রোগ্রামটি স্বয়ংক্রিয়ভাবে অ্যাপ্লিকেশন সার্ভারের সঙ্গে সংযুক্ত হয়ে যায়। অ্যাপ্লিকেশন সার্ভার ব্যবহারকারীর সঙ্গে বিভিন্ন মেনু, সাব-মেনু, প্রম্পট, উইন্ডো ইত্যাদি প্রদান করে এবং তথ্য ও নির্দেশনা সংগ্রহ করে। অবশেষে নির্দেশাবলি কার্যকর করার জন্য, তথ্যসমূহ ডাটাবেস সার্ভারে হস্তান্তর করা হয়।

#### গ. ডাটাবেস সার্ভার

ডাটাবেস সার্ভার গ্রাহকের তথ্য সংরক্ষণ করে। এটি গ্রাহকের ডেটা পরিবর্তন করার আগে কিছু ব্যবসায়িক নিয়ম এবং ধারাবাহিকতা যাচাই করে। ডেটাবেস সার্ভার গ্রাহকের ডেটা পরিবর্তন করার জন্য অ্যাপ্লিকেশন সার্ভার থেকে নির্দেশনা পায়। এটি কিছু ব্যবসায়িক নিয়মকে যাচাই করে যেমন অ্যাকাউন্টে টাকা তোলার জন্য পর্যাপ্ত ব্যালেন্স আছে কি না, চেকের পাতা ব্যবহার করে পূর্বে পেমেন্ট করা হয়েছে কি না, ইত্যাদি। বৈধতা পাস হলে, ডাটাবেস সার্ভার অ্যাকাউন্টের অবস্থা আপডেট করে এবং লেনদেন সংরক্ষণ করে।

### ৩.১.২. রেইড (RAID)

রেইডের অর্থ হলো রিডান্ড্যান্ট অ্যারে অব ইনডিপেনডেন্ট ডিস্ক এবং তাহা একাধিক হার্ড ডিস্ক সংবলিত অভ্যন্তরীণ স্টোরেজ বা ডেটা নির্ভরযোগ্যতা বাড়ানোর জন্য বাহ্যিক স্টোরেজ সিস্টেমে ব্যবহৃত হয়।

রেইড হলো একটি প্রযুক্তি, যা কম্পিউটার সার্ভারের হার্ড ড্রাইভের জন্য ডেটা নির্ভরযোগ্যতা প্রদান করতে এবং ইনপুট/আউটপুট কর্মক্ষমতা বাড়াতে ব্যবহৃত হয়। যখন একাধিক ফিজিক্যাল ডিস্ক রেইড প্রযুক্তি ব্যবহার করার জন্য সেট আপ করা হয়, তখন সেগুলোকে রেইড অ্যারেতে রয়েছে বলা হয়। এই অ্যারে একাধিক ডিস্কজুড়ে ডেটা সংরক্ষণ করে, কিন্তু অ্যারেটিকে কম্পিউটার ব্যবহারকারী এবং অপারেটিং সিস্টেম একটি একক ডিস্ক হিসাবে দেখতে পায়।

বিভিন্ন রেইড স্তর রয়েছে—

লেভেল ০ : ত্রুটি সহনশীলতা ছাড়াই স্ট্রাইপড ডিস্ক অ্যারে (Striped Disk Array without Fault Tolerance) : ইহা ডেটা স্ট্রিপিং প্রদান করে (একাধিক ডিস্ক ড্রাইভজুড়ে প্রতিটি ফাইলের ব্লক ছড়িয়ে দেয়) কিন্তু এতে কোনো রিডান্ডেন্সি নেই। এটি কর্মক্ষমতা উন্নত করে কিন্তু দোষ সহনশীলতা প্রদান করে না। একটি ড্রাইভ ফেইল হলে অ্যারের সমস্ত ডেটা হারিয়ে যায়।

লেভেল ১ : মিরোরিং এবং ডুপ্লেক্সিং (Mirroring and Duplexing) : ইহা ডিস্ক মিরোরিং প্রদান করে। মিরোরিং হলো এমন একটি কৌশল যেখানে ডেটা একই সঙ্গে দুটি ডিস্কে লেখা হয়। এইভাবে যদি একটি ডিস্ক ড্রাইভ ফেইল হয়, সিস্টেমটি তাৎক্ষণিকভাবে ডেটা বা পরিষেবার কোনো ক্ষতি ছাড়াই অন্য ডিস্কে সুইচ করতে পারে।

লেভেল ২ : ত্রুটি-সংশোধন কোডিং (Error Correcting Coding) : এটি সাধারণ বাস্তবায়ন করতে দেখা যায় না অর্থাৎ খুব কমই ব্যবহৃত হয়। লেভেল ২ পদ্ধতিতে, ডেটা সাধারণত ব্লক লেভেলের পরিবর্তে বিট লেভেলে লিখে থাকে।

লেভেল ৩ : বিট-ইন্টারলিভড প্যারিটি (Bit Interleaved Parity) : এটি ডেডিকেটেড প্যারিটি ডিস্কের সঙ্গে বাইট-লেভেল ডেটা লিখে থাকে। লেভেল ৩ একযোগে একাধিক অনুরোধ গ্রহণ করতে পারে না, তাই এটি খুব কমই ব্যবহৃত হয়।

লেভেল ৪ : ডেডিকেটেড প্যারিটি ড্রাইভ (Dedicated Parity Drive) : এটি একটি সাধারণভাবে ব্যবহৃত ও বাস্তবায়িত রেইড লেভেল। লেভেল ৪ একটি প্যারিটি ডিস্কসহ ব্লক-লেভেল-এ (যেমন লেভেল ০) ডেটা লিখতে পারে। যদি একটি ডেটা ডিস্ক ফেইল করে, তখন একটি প্রতিস্থাপন ডিস্ক তৈরি করতে প্যারিটি ডেটা ব্যবহৃত হয়। লেভেল ৪ এর একটি অসুবিধা হলো প্যারিটি ডিস্ক লেখার ক্ষেত্রে যদি বাধার সৃষ্টি হয়, তখন ডেটা রিকভার করা সম্ভব হয় না।

লেভেল ৫ : ব্লক ইন্টারলিভড ডিস্ট্রিবিউটেড প্যারিটি (Block Interleaved Distributed Parity) : এটি বাইট লেভেলে ডাটা লেখাতে ও ভুল সংশোধন করতে সাহায্য করে। এটির কর্মক্ষমতা চমৎকার এবং ভালো দোষ সহনশীলতা রয়েছে। লেভেল ৫ হলো রেইডের অন্যতম জনপ্রিয় একটি লেভেল।

লেভেল ৬ : ডাবল প্যারিটিসহ ইনডেপেন্ডেন্ট ডেটা ডিস্ক (Independent Data Disks with Double Parity) : ইহা সমস্ত ডিস্কে বিতরণ করা প্যারিটিসহ ব্লক-লেভেল-এ ডেটার স্ট্রিপিং প্রদান করে।

লেভেল ০+১- মিরোর অব স্ট্রাইপস্ (A Mirror of Stripes) : এটি মূল রেইড স্তরগুলোর একটি নয়। এখানে দুটি রেইড ব্যবহার করা হয়েছে—প্রথমে ০ স্ট্রাইপ তৈরি করা হয়েছে এবং তাদের ওপর রেইড ১ মিরোর তৈরি করা হয়েছে। ডিস্কের মধ্যে ডেটা রেপ্লিক্যাট ও শেয়ার করার জন্য এটি ব্যবহৃত হয়।

### ৩.১.৩. ক্লাস্টারিং (Clustering)

ক্লাস্টারিং হলো সংযুক্ত কম্পিউটার সার্ভারগুলোর একটি গ্রুপিং, একসঙ্গে কাজ করে যাতে অনেক ক্ষেত্রে তারা একটি একক কম্পিউটার সার্ভার গঠন করে। দুটি কম্পিউটারের মধ্যে একটি ক্লাস্টার তৈরির উদ্দেশ্যের ওপর ভিত্তি করে, ক্লাস্টারিং নিম্নলিখিত ধরনের হতে পারে :

#### ক. হাই অ্যাভেইলেবল (এইচএ) ক্লাস্টার

হাই অ্যাভেইলেবল ক্লাস্টারগুলো (ফেলওভার ক্লাস্টার নামেও পরিচিত) প্রাথমিকভাবে পরিষেবাগুলোর প্রাপ্যতা নিশ্চিত করার উদ্দেশ্যে ব্যবহার করা হয়। এখানে দুটি নোড (সার্ভার)-এর মধ্যে একটি রিডান্ড্যান্ট নোড থাকে, যা প্রথমটি ফেইল করলে ব্যবহৃত হয়। একটি এইচএ ক্লাস্টারের জন্য সবচেয়ে ছোট আকারের ক্লাস্টার হলো দই নোড ক্লাস্টার, যাহা সর্বনিম্ন রিডানডেন্সির জন্য প্রয়োজন। এইচএ ক্লাস্টার 'সিঙ্গল পয়েন্ট অব ফেইলিউর' দূর করার জন্য প্রয়োজনীয় রিডানডেন্সি প্রদান করে থাকে। এটিকে একটি এক্টিভ প্যাসিভ (Active-Passive) ক্লাস্টারও বলা হয়।

#### খ. লোড-ব্যালেন্সিং ক্লাস্টার

একটি লোড-ব্যালেন্সিং ক্লাস্টারে, প্রতিটি ৫০% লোডে দুটি কম্পিউটার একসঙ্গে সংযুক্ত থাকে এবং এগুলো একত্রে একটি একক ভার্চুয়াল কম্পিউটার হিসাবে কাজ করে। ব্যবহারকারীর কাছ থেকে পাওয়া অনুরোধ একটি নেটওয়ার্ক লোড ব্যালেন্সার দ্বারা দুটি কম্পিউটারের মধ্যে বিতরণ করা হয়। ফলে বিভিন্ন কম্পিউটারের মধ্যে সমভাবে কাজের বণ্টন নিশ্চিত হয়। ফলে একদিকে ক্লাস্টার

সিস্টেমের কর্মক্ষমতা উন্নত করে এবং অন্যদিকে রিডানডেন্সি প্রদান করে অর্থাৎ একটি নোড ব্যর্থ হলে অন্য নোড ১০০% লোডে চলতে পারে। এটিকে একটি এক্টিভ-এক্টিভ (Active-Active) ক্লাস্টারও বলা হয়।

### ৩.১.৪. রেপ্লিকেশন (Replication)

রেপ্লিকেশন হলো এক ডাটাবেস থেকে অন্য ডাটাবেসে ডেটা এবং ডাটাবেস অবজেক্টে কপি করা এবং তারপরে দুটি ডেটাবেজের মধ্যে ধারাবাহিকতা বজায় রাখার জন্য ব্যবহৃত প্রযুক্তি। রেপ্লিকেশন পদ্ধতি ব্যবহার করে ডেটা দূরবর্তী কোনো লোকেশনে, সাধারণত ডেটা সেন্টার থেকে ডিআরএস-এ, কপি করা হয়। এতে হাই স্পিড লিংকের প্রয়োজন হয়। রেপ্লিকেশন অসিঙ্ক্রোনাস (অ্যাসিঙ্ক) বা সিঙ্ক্রোনাস (সিঙ্ক) হতে পারে।

#### ক. অ্যাসিঙ্ক রেপ্লিকেশন (Async Replication)

একটি অ্যাসিঙ্ক রেপ্লিকেশন একটি নির্ধারিত সময় পর পর, যেমন ৫ মিনিটের একটি নির্দিষ্ট সময়ের ব্যবধানে ডেটা ডিসি থেকে ডিআরএস-এ স্থানান্তরিত হয়। ফাইবার অপটিক সংযোগ ব্যবহার করে এই ধরনের রেপ্লিকেশন তৈরি করা যেতে পারে। সিস্টেম ফেইল হলে গত ৫ মিনিটের ডেটা পাওয়া না যেতে পারে।

#### খ. সিঙ্ক রেপ্লিকেশন (Sync Replication)

একটি সিঙ্ক রেপ্লিকেশনে, ডাটা তাৎক্ষণিকভাবে ডিসি থেকে ডিআরএস-এ স্থানান্তরিত হয়, যার অর্থ, যখনই লেনদেন ডিসি-তে রেকর্ড করা হলে, তখনই তাহা সঙ্গে সঙ্গে ডিআরএস-এ রেকর্ড করা হয়। সিঙ্ক রেপ্লিকেশনের জন্য একটি ডার্ক ফাইবার প্রয়োজন।

### ৩.১.৫. ডার্ক ফাইবার (Dark Fiber)

একটি ডার্ক ফাইবার হলো দুটি বিন্দুর মধ্যে একটি নিবেদিত সরাসরি ফাইবার অপটিক লিঙ্ক। সাধারণত ডিসি ও ডিআরএস-এর মধ্যে ডেটার রেপ্লিকেশনের জন্য এটি ব্যবহৃত হয়। ডার্ক ফাইবারগুলো ভাগাভাগি করে ব্যবহার করা যায় না এবং ডার্ক ফাইবারের দুই প্রান্তে কোনো রাউটার সংযুক্ত থাকে না (ফলে যোগাযোগের জন্য টিসিপি/আইপি প্রোটোকল ব্যবহার করা হয় না)। তাদের ব্যান্ডউইথ খুব বেশি এবং ডেটা ট্রান্সমিশনের গতি খুব দ্রুত।

### ৩.১.৬. এক্সটার্নাল স্টোরেজ সিস্টেম (External Storage System)

একটি ব্যাংকে, ডেটার পরিমাণ বিশাল যা একটি কম্পিউটার সার্ভারের অভ্যন্তরীণ হার্ড ডিস্কগুলো ধারণ করতে পারে না। গ্রাহকের তথ্য সংরক্ষণ করতে এবং প্রতিদিনের লেনদেন রেকর্ড করতে ৫০-৫০০ টি হার্ডডিস্কের প্রয়োজন। একটি এক্সটার্নাল স্টোরেজ ডিভাইসে এই সব হার্ড ডিস্ক স্থাপন করা হয়। ডিভাইসটিতে হার্ডডিস্ক পরিচালনা করার জন্য প্রসেসর, র‍্যাম, সফ্টওয়্যার ইত্যাদিও রয়েছে যাতে বিভিন্ন সার্ভারে চলমান বিভিন্ন অ্যাপ্লিকেশনের জন্য স্থান বরাদ্দ করা যায়। কাজেই এক্সটার্নাল স্টোরেজ সিস্টেম, স্টোরেজ একত্রীকরণের (Storage Consodilation) জন্যও ব্যবহার করে। এই ধরনের স্টোরেজ সিস্টেমে ডেটা সেন্টার থেকে ডিআরএস-এ ডেটা রেপ্লিকেশন করার ক্ষমতা রয়েছে।

### ৩.১.৭. স্যান সুইচ (SAN Switch)

এক্সটার্নাল স্টোরেজ ডিভাইসটি স্যান সুইচের মাধ্যমে সার্ভারের সঙ্গে সংযুক্ত থাকে। স্যান হলো স্টোরেজ এরিয়া নেটওয়ার্ক। এটি সার্ভার ও স্টোরেজ ডিভাইস সমন্বয়ে গঠিত একটি উচ্চ-গতির নেটওয়ার্ক।

## ৩.২. ডাটাবেস ব্যাকআপ সিস্টেম (Databse Backup system)

ডাটাবেস গ্রাহক ও তাদের লেনদেন এবং ক্রেডিট কার্ড সম্পর্কিত গুরুত্বপূর্ণ তথ্য সংরক্ষণ করে। ক্ষতি থেকে এই তথ্য রক্ষা করা খুবই গুরুত্বপূর্ণ। ডাটাবেস ব্যাকআপ হলো ডাটাবেস রক্ষা এবং পুনরুদ্ধার করার একটি উপায়। সাধারণত, ডাটাবেস ব্যাকআপ আরডিবিএমএস (RDBMS) বা অনুরূপ ডাটাবেস ম্যানেজমেন্ট সফ্টওয়্যার দ্বারা তৈরি করা হয়। বিপর্যয়ের ক্ষেত্রে, ডাটাবেস অ্যাডমিনিস্ট্রেটর (ডিবিএ) ডাটাবেস ব্যাকআপ কপি থেকে সমস্ত ডেটা এবং লগ পুনরুদ্ধার করতে পারেন। ডাটাবেস ব্যাকআপ স্থানীয়ভাবে বা ব্যাকআপ সার্ভারে বা ক্লাউডে রাখা যেতে পারে।

ব্যবসায়িক এবং সরকারি আদেশের প্রতিপালন করতে, এবং দুর্যোগ বা প্রযুক্তিগত বিভ্রাটের ক্ষেত্রে গুরুত্বপূর্ণ ব্যবসায়িক ডেটা পুনরুদ্ধার করতে ডেটাবেস ব্যাকআপ নিতে হয়।

### ডাটাবেস ব্যাকআপের ধরন

#### ক. ফুল ব্যাকআপ (Full Backup)

ফুল ব্যাকআপ হলো একটি মৌলিক কিন্তু পরিপূর্ণ একটি ব্যাকআপ পদ্ধতি। নাম থেকে বোঝা যায়, এই ধরনের ব্যাকআপ সমস্ত ডেটার একটি কপি স্টোরেজ ডিভাইস যেমন একটি ডিস্ক বা টেপ-এ তৈরি করে। একটি ফুল ব্যাক আপের সুবিধা হলো যে, প্রতি ব্যাক আপের পর একটি ডিভাইসেই সম্পূর্ণ ডেটা পাওয়া যায়। এর ফলে ডেটা পুনরুদ্ধার করার জন্য কম সময়ের প্রয়োজন হয়। কিন্তু অসুবিধাগুলো হলো যে এটি ধারণ করতে অন্যান্য ধারণের ব্যাকআপের চেয়ে বেশি

(প্রায় ১০ গুণ বা তার চেয়েও বেশি) সময় লাগে এবং এটির জন্য বেশি স্টোরেজ স্পেস এর প্রয়োজন হয়।

তাই ফুল ব্যাকআপগুলো সাধারণত মাঝে মাঝে চালানো হয়। যে সমস্ত ডেটা সেন্টারগুলোতে অল্প পরিমাণে ডেটা (বা গুরুত্বপূর্ণ অ্যাপ্লিকেশন) রয়েছে সেখানে প্রতিদিন একটি ফুল ব্যাকআপ নেওয়া যেতে পারে, বা কিছু ক্ষেত্রে আরও ঘন ঘন নেওয়া যেতে পারে। সাধারণত, ইনক্রিমেন্টাল বা ডিফারেনশিয়াল ব্যাকআপগুলোর সঙ্গে মিলিয়ে একটি ফুল ব্যাকআপ নেওয়া হয়। এ ধরনের ব্যাকআপের ক্ষেত্রে পুনরুদ্ধার কার্যক্রম সহজ হয় এবং এর জন্য কম সময় লাগে, কারণ শুধু সর্বশেষ ব্যাকআপ থেকেই ডেটা সম্পূর্ণ পুনরুদ্ধার করা যায়।

### খ. ইনক্রিমেনটাল ব্যাকআপ (Incremental Backup)

ইনক্রিমেনটাল ব্যাকআপ পদ্ধতিতে সর্বশেষ ব্যাকআপের পর থেকে অদ্যাবধি যে সমস্ত পরিবর্তন হয়েছে শুধু তাই কপি করা হয়। প্রতিটি ফাইলে টাইম স্ট্যাম্প ব্যবহার করা হয় এবং তা সর্বশেষ ব্যাকআপের টাইম স্ট্যাম্পের সঙ্গে তুলনা করা হয়। ব্যাকআপ এপ্লিকেশন এ কাজটি করে থাকে।

যেহেতু একটি ইনক্রিমেন্টাল ব্যাকআপ শুধু শেষ ব্যাকআপের পর থেকে শুরু করে ডেটা কপি করে, তাই একটি সংস্থা এটিকে যতবার ইচ্ছা ততবার চালাতে পারে। এতে শুধু সাম্প্রতিক পরিবর্তনগুলো কপি করা হয়। একটি ইনক্রিমেন্টাল ব্যাকআপের সুবিধা হলো যে এটি একটি ফুল ব্যাকআপের তুলনায় অল্প পরিমাণ ডেটা কপি করে। ফলে, এতে ব্যাকআপ দ্রুত গতিতে সম্পন্ন হয়, এবং ব্যাকআপ কপি করার জন্য কম জায়গার প্রয়োজন হবে। ডেটা পুনরুদ্ধার অপারেশনের জন্য প্রথম দিনের ফুল ব্যাকআপ এবং পরবর্তী ইনক্রিম্যান্টাল ব্যাকআপগুলোর প্রয়োজন হয়। কিন্তু ডেটা পুনরুদ্ধারের সময় বেশি সময় লাগে এবং প্রতিটি ইনক্রিমেন্টাল ব্যাকআপের কপি সঠিকভাবে কাজ করতে হবে। একটি ব্যাকআপ কাজ না করলে সমগ্র পুনরুদ্ধারকে প্রভাবিত করতে পারে।

### গ. ডিফারেনশিয়াল ব্যাকআপ (Differential Backup)

একটি ডিফারেনশিয়াল ব্যাকআপ অপারেশন প্রথমবার ডেটার ফুল ব্যাকআপ নেয় এবং পরবর্তী ব্যাকআপগুলো ঐ ব্যাকআপ থেকে পরিবর্তীত সমস্ত ডেটা অনুলিপি করবে। এইভাবে, এটি পরবর্তী ব্যাকআপগুলোতে ইনক্রিমেন্টাল ব্যাকআপের চেয়ে বেশি ব্যাকআপ ডেটা সংরক্ষণ করবে, যদিও এটিতে একটি ফুল ব্যাকআপের তুলনায় অনেক কম ডেটা সংরক্ষণ করতে হয়। তাছাড়া একটি ডিফারেনশিয়াল ব্যাকআপ তৈরি করতে ইনক্রিমেন্টাল ব্যাকআপের চেয়ে বেশি জায়গা ও সময়ের প্রয়োজন হয়, যদিও তা ফুল ব্যাকআপের চেয়ে অনেক কম।

একটি ডিফারেনশিয়াল ব্যাকআপ থেকে ডেটা পুনরুদ্ধারের জন্য শুধু প্রথম ফুল ব্যাকআপ ও শেষ ডিফারেনশিয়াল ব্যাকআপের প্রয়োজন হয়। এতে পুনরুদ্ধারের জন্য সময় কম লাগে এবং অনেকগুলো ব্যাকআপ না থাকায়, অকার্যকর ব্যাকআপ মিডিয়াজনিত সমস্যা কম হয়।

## ৪. এফআই কম্পিউটারাইজেশন পদ্ধতি

ব্যাংকিং কার্যক্রমের স্বয়ংক্রিয়করণের বিভিন্ন পদ্ধতি রয়েছে। প্রাথমিক স্বয়ংক্রিয়তা ব্যাংকগুলোতে একক কম্পিউটার ব্যবহারের মাধ্যমে শুরু হয়। এরপর ধীরে ধীরে বিভিন্ন ব্যাংকে ল্যান, ডিস্ট্রিবিউটেড ডাটাবেসসহ ওয়্যান এবং সেন্ট্রালাইজড ডাটাবেসসহ ওয়্যান চালু করা হয়। একটি সেন্ট্রালাইজড ডাটাবেসের প্রবর্তন ব্যাংকগুলোকে ই-ব্যাংকিং শুরু করতে সহায়তা করে। ই-ব্যাংকিং এর মধ্যে রয়েছে বিভিন্ন ইলেকট্রনিক ব্যাংকিং চ্যানেল এর সমাহার যেমন এটিএম, পিওএস, ইন্টারনেট ব্যাংকিং, এসএমএস এবং অ্যালার্ট ব্যাংকিং, ই-কমার্স, এম-কমার্স এবং কল সেন্টার। এই ইলেকট্রনিক চ্যানেলগুলো ব্যবহার করে, ব্যাংকগুলো তাদের গ্রাহকদের বিভিন্ন ব্যাংকিং পরিষেবা দিতে পারে। এই ইলেকট্রনিক চ্যানেলগুলোকে সম্মিলিতভাবে অল্টারনেটিভ ডেলিভারি চ্যানেলও বলা হয়। কিছু কিছু বিকল্প ডেলিভারি চ্যানেল ব্যবহার করতে গ্রাহকের একটি প্লাস্টিকের কার্ড প্রয়োজন। প্লাস্টিক কার্ডটি ডেবিট কার্ড, ক্রেডিট কার্ড বা প্রিপেইড কার্ড হতে পারে। এই কার্ডগুলো সম্মিলিতভাবে প্লাস্টিক মানি নামে পরিচিত। প্লাস্টিক কার্ডের উৎপাদন ও পরিচালনার জন্য, ব্যাংকগুলোকে বিভিন্ন সফ্টওয়্যার ইনস্টল করতে হয় এবং কিউ-ক্যাশ, মাস্টরকার্ড ও ভিসা কার্ডের মতো বিভিন্ন স্থানীয় ও আন্তর্জাতিক পেমেন্ট অ্যাসোসিয়েশনের সদস্য হতে হয়। নিম্নলিখিত অনুচ্ছেদগুলোতে ব্যাংক অটোমেশনের বিভিন্ন পদ্ধতির বর্ণনা করা হলো। পরবর্তী অধ্যায়গুলোতে প্লাস্টিক মানি এবং অল্টারনেটিভ ডেলিভারি চ্যানেল নিয়ে আলোচনা করা হবে।

### ৪.১. স্ট্যান্ড-এলোন সিস্টেম (Stand-alone System)

আশির দশকে, বাংলাদেশের ব্যাংকগুলো কেবলমাত্র গ্রাহকদের লেজার প্রতিস্থাপনের জন্য কম্পিউটারাইজেশন শুরু করে। গ্রাহকদের লেজার বা খাতা প্রতিস্থাপনের জন্য ব্যবহৃত সফ্টওয়্যারটি ব্যাংক কাউন্টারে অর্থ প্রাপ্তি এবং অর্থপ্রদানের সময় গ্রাহকের অ্যাকাউন্টে ডেবিট এবং ক্রেডিট এন্ট্রি পোস্ট করার জন্য শাখা দ্বারা ব্যবহৃত হতো। এসব সফ্টওয়্যার অন্য কোনো ব্যাংকিং কার্যক্রম যেমন ক্রেডিট এবং বৈদেশিক বাণিজ্য এবং ব্যাক অফিসের কার্যক্রম যেমন সুদের গণনা, সার্ভিস চার্জ, ফি এবং কমিশন, জেনারেল লেজার রক্ষণাবেক্ষণ, চার্ট অব

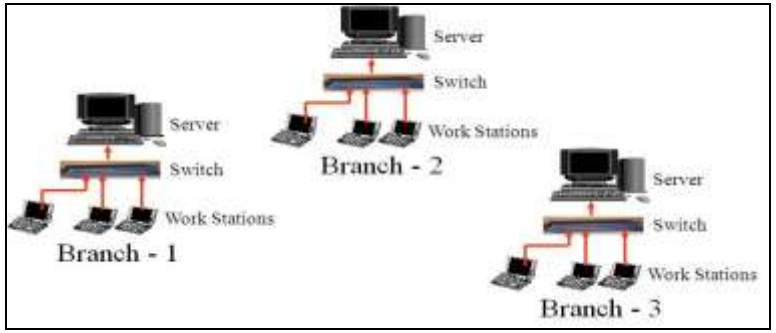
অ্যাকাউন্ট প্রস্তুত করা, আয়-ব্যয়ের বিবরণী এবং অন্যান্য প্রতিবেদন অন্তর্ভুক্ত করা হয়নি।

সফ্‌টওয়্যারটি স্ট্যান্ট-অ্যালোন ছিল অর্থাৎ এটি একাধিক কম্পিউটার দ্বারা একসঙ্গে ব্যবহার করা যেত না। এটি একটি শাখার একটি কম্পিউটারে ইনস্টল করা হতো। ডাটা এন্ট্রির জন্য একজন কম্পিউটার অপারেটর পদায়ন করা হতো। ব্যাংকের টেলার গ্রাহককের কাছ থেকে চেকটি গ্রহণ করেন এবং পোস্ট করার জন্য কম্পিউটার অপারেটরের কাছে পাঠান। পোস্টিং সফলভাবে করার পরে, টেলার গ্রাহকের কাছে টাকা হস্তান্তর করেন। কিন্তু, টাকা জমা দেওয়ার রসিদ ভাউচারগুলো লেনদেনের সময় শেষ হওয়ার পরেও পোস্ট করা হতো।

স্ট্যান্ড-অ্যালোন সিস্টেমের বড় অসুবিধা হলো যে এটি বড় শাখার জন্য ব্যবহার করা যাবে না যেখানে লেনদেনের সংখ্যা প্রচুর। আরেকটি অসুবিধা হলো এই সিস্টেমে সমস্ত ব্যাংকিং কার্যকারিতার অনুপস্থিতি। বেক্সিমকো কম্পিউটারস 'বেক্সিব্যাংক' নামে বাংলাদেশে প্রথম স্ট্যান্ড-অ্যালোন ব্যাংকিং সফ্‌টওয়্যার তৈরি করে।

### ৪.২. ল্যান-ভিত্তিক সিস্টেম (LAN-based System)

নব্বইয়ের দশকে, ল্যান-ভিত্তিক কোর ব্যাংকিং সফটওয়্যারটি আবিষ্কৃত হয়। একটি ল্যান-ভিত্তিক সিস্টেমে, সফ্‌টওয়্যারটি একটি কম্পিউটার সার্ভারে ইনস্টল করা হয়েছিল। কম্পিউটার সার্ভার একটি হাব বা নেটওয়ার্ক সুইচের সঙ্গে সংযুক্ত ছিল। ওয়ার্কস্টেশন নামে অন্য সব কম্পিউটার এই হাব বা নেটওয়ার্ক সুইচের মাধ্যমে সার্ভারের সঙ্গে সংযুক্ত ছিল। টেলার এবং ব্যাক অফিস অফিসারদের প্রত্যেককে পোস্টিংয়ের জন্য একটি ওয়ার্কস্টেশন দেওয়া হতো। সমস্ত গ্রাহক এবং অ্যাকাউন্ট সম্পর্কিত তথ্য এবং লেনদেন সার্ভারের সঙ্গে হার্ড ডিস্কে রেকর্ড করা হতো।




*একটি ল্যান-ভিত্তিক কোর ব্যাংকিং সিস্টেম*

কম্পিউটারসমূহের মধ্যে ল্যান স্থাপনের জন্য ইউনিক্স বা নভেল অপারেটিং সিস্টেম ব্যবহার করা হতো। ডেটা, সার্ভারে অবস্থিত একটি ফ্ল্যাট ফাইল বা ডাটাবেসে সংরক্ষণ করা হতো—যাহা ফক্সপ্রো বা ডিবেস নামে পরিচিত ছিল। অ্যাপ্লিকেশন সফ্‌টওয়্যারটি কোবল, ফক্সপ্রো বা ডিবেইজ-এ লেখা হতো।

ল্যান-ভিত্তিক কোর ব্যাংকিং সফটওয়্যারটি বাংলাদেশের বিভিন্ন কোম্পানি দ্বারা তৈরি করা হয়েছে, যার একটি তালিকা নিচে দেওয়া হলো—

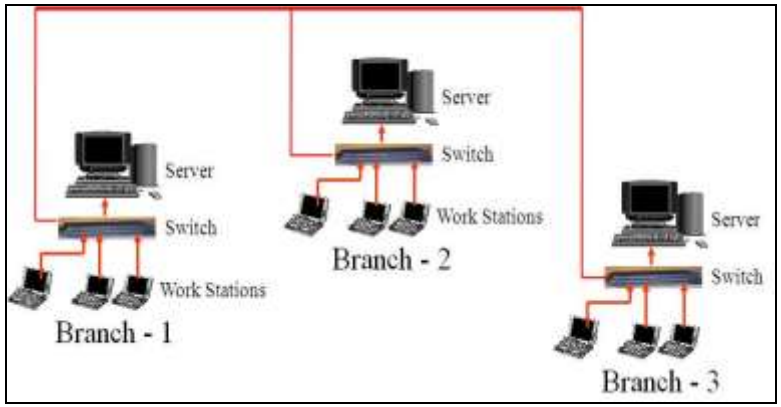
| ক্রম. | সফটওয়্যারের নাম | ডেভেলপারের নাম |
|---|---|---|
| ১ | পিসিব্যাংক<br>পিসিব্যাংক/এম<br>পিসিব্যাংক ২০০০ | লিডস কর্পোরেশন লিমিটেডের |
| ২ | বেক্সিব্যাংক৩০০০,<br>বেক্সিব্যাংক৩০০০+<br>বেক্সিব্যাংক ৪০০০<br>বেক্সিব্যাংক ৫০০০ | বেক্সিমকো কম্পিউটারস লি. |
| ৩ | এ -জেড ব্যাংকিং সফটওয়্যার | এ টু জেড কম্পিউটার লিমিটেড |
| ৪ | ইজব্যাংক (Ease Bank) | কম্পিউটার ইজ লিমিটেড |
| ৫ | আইবিএস (IBS) | ইনফিনিটি টেকনোলজি ইন্টারন্যাশনাল লি. |
| ৬ | ই-ব্যাংকিং | ডেস্কটপ কম্পিউটার কানেকশন লি. |
| ৭ | কার্নেল (Karnel) | কার্নেল সফটওয়্যার লিমিটেড |
| ৮ | ফ্লোরাব্যাংক | ফ্লোরা লিমিটেড |
| ৯ | মিলিনিয়াম | সাউথটেক লিমিটেড |
| ১০ | টিআইবিএস (TIBS) | টেকনোহেভেন লিমিটেড |

ল্যান-ভিত্তিক সফ্‌টওয়্যারটিতে, অনেকগুলো ব্যাংকিং বৈশিষ্ট্য অন্তর্ভুক্ত ছিল। কিন্তু অ্যাকাউন্টধারীদের ডেটা শুধু একটি শাখায় সংরক্ষিত থাকত এবং একমাত্র ঐ শাখা থেকেই তা এক্সেস করা যেত। ফলে এই ধরনের সফ্‌টওয়্যার ব্যবহার করে অনলাইন ব্যাংকিং চালু করা সম্ভব ছিল না।

কিন্তু এই ধরনের সফ্‌টওয়্যারের খরচ খুবই কম ছিল, যা প্রতি শাখার জন্য মাত্র ৫০,০০০ – ৭০,০০০ টাকা ছিল।

### ৪.৩. ডিস্ট্রিবিউটেড ডাটাবেসসহ ওয়্যান-ভিত্তিক সিস্টেম (WAN-based System with distributed database)

২০০০ সালে, বাংলাদেশ টেলিফোন অ্যান্ড টেলিগ্রাম বোর্ড (বিটিটিবি) তার মগবাজার এক্সচেঞ্জে ডিডিএন (ডিজিটাল ডেটা নেটওয়ার্ক) সুইচ ইনস্টল করে। ডিডিএন হলো একটি ডেটা কমিউনিকেশন মিডিয়া, যা সাধারণ টেলিফোন লাইন ব্যবহার করে সর্বোচ্চ ২৫৬ কেবিপিএস গতিতে কাজ করে। এটি বাংলাদেশের সকল জেলা শহরে পাওয়া যেত। এই যোগাযোগ মাধ্যম ব্যবহার করে, কিছু ব্যাংক জেলা শহরে শাখাগুলোর মধ্যে ওয়্যান স্থাপন শুরু করে।




*ডিস্ট্রিবিউটেড ডাটাবেসসহ একটি ওয়্যান-ভিত্তিক কোর ব্যাংকিং সিস্টেম*

এভাবে প্রতিষ্ঠিত ওয়্যান বিভিন্ন শাখায় প্রতিষ্ঠিত ল্যানসমূহকে একত্রে সংযোগ করতে সক্ষম হয়েছিল। ফলে গ্রাহককে অন্য শাখায় গিয়ে অর্থ উত্তোলন বা জমা করার সুবিধা প্রদান করেছিল। এটি সেমি-অনলাইন ব্যাংকিংয়ের যুগ সূচনা করে। এই পদ্ধতিতে অন্য শাখা থেকে ব্যাংকিং করার জন্য গ্রাহককে সেই শাখাগুলোর নাম ঘোষণা করতে হবে যেখান থেকে তিনি অনলাইন পরিষেবা পেতে চান। গ্রাহকের হোম শাখা গ্রাহকের স্বাক্ষর কার্ড এবং ফটোগ্রাফের কপি তৈরি করে এবং তা ঐ সব শাখায় পাঠিয়ে দেয়, যা দেখে ঐ শাখার টেলার গ্রাহকের পরিচিতি নিশ্চিত করে। অন্যান্য শাখার টেলাররা ওয়্যান সংযোগ এবং একটি বিশেষ পাসওয়ার্ড ব্যবহার করে গ্রাহকের হোম ব্রাঞ্চের সার্ভারে প্রবেশ করে এবং পোস্টিং সম্পন্ন করে।

ওয়্যান-ভিত্তিক সফ্টওয়্যারটি ল্যান-ভিত্তিক লেনদেনের জন্য ব্যবহৃত সফ্টওয়্যারটির মতোই, তাতে শুধু অন্য শাখা থেকে লেনদেন গ্রহণ করার জন্য সামান্য কাস্টমাইজেশন করা হয়েছে।

তবে, এই সিস্টেমটি অনলাইন ব্যাংকিংয়ের জন্য একটি সম্পূর্ণ সমাধান হিসাবে বিবেচিত হয়নি। এই সিস্টেমটিতে বিভিন্ন ডেলিভারি চ্যানেল যেমন এটিএম, পিওএস, ইন্টারনেট ব্যাংকিং সিস্টেম, এসএমএস বা অ্যালার্ট ব্যাংকিং সিস্টেমের ব্যবহার সম্ভব হতো না। এই সিস্টেমটি ব্যবহার করে, যদি কোনো ব্যাংক এটিএমগুলো অন্তর্ভুক্ত করতে চায়, তবে তার সমস্ত শাখাগুলোর সার্ভার দিনে ২৪ ঘণ্টা এবং সপ্তাহে ৭ দিন খোলা রাখতে হবে। এটি সম্ভব নয়, কারণ এরকম সার্ভারগুলো ২৪ ঘণ্টা অপারেশনের জন্য তৈরি করা হয় না এবং অন্যান্য অনেক কারণ যেমন বিশেষজ্ঞ জনবল, সঠিক বৈদ্যুতিক শক্তি এবং পর্যাপ্ত শীতাতপ নিয়ন্ত্রণ ব্যবস্থা সমস্ত শাখায় সম্ভব নাও হতে পারে।

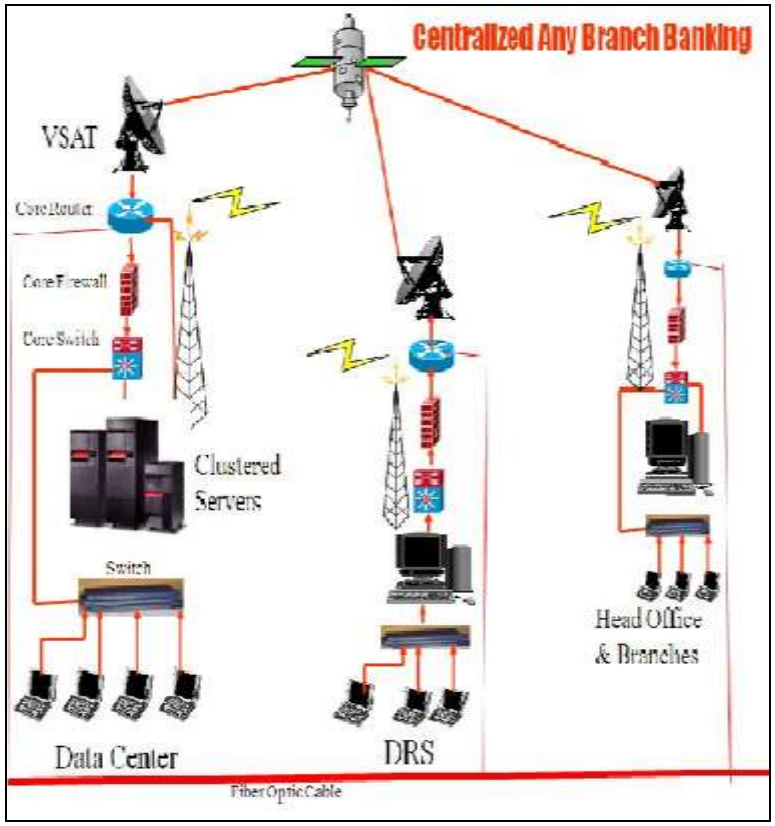
একটি সেন্ট্রালাইজড কোর ব্যাংকিং সিস্টেম ইনস্টল করার মাধ্যমে সত্যিকারের অনলাইন ব্যাংকিং অর্জন করা যেতে পারে। স্থানীয় ব্যাংকগুলোর মধ্যে, এবি ব্যাংক, সেই সময়ে, 'ইকুয়েশন' নামে একটি কেন্দ্রীভূত কোর ব্যাংকিং সিস্টেম ঐ সময় ব্যবহার করত। তবে, শুধু ঢাকা শহরের শাখাগুলো এই সেন্ট্রালাইজড কোর ব্যাংকিং ব্যবস্থার সঙ্গে যুক্ত ছিল।

### ৪.৪. একটি সেন্ট্রালাইজড ডাটাবেসসহ ওয়্যান-ভিত্তিক সিস্টেম (WAN-based System with Centralized Database)

২০০৪ সালে, ইস্টার্ন ব্যাংক, ঢাকা ব্যাংক, এবং ডাচ্-বাংলা ব্যাংক দ্বারা একযোগে সেন্ট্রালাইজড কোর ব্যাংকিং সিস্টেম ইনস্টল করা হয়েছিল। তিনটি ব্যাংকই আই-ফ্ল্যাক্স সলুশনস লিমিটেড, ভারত থেকে 'ফ্লেক্সকিউব' নামে একটি কোর ব্যাংকিং সফ্টওয়্যার সংগ্রহ করেছে। ব্যাংকের 'ডেটা সেন্টারে' কেন্দ্রীয়ভাবে সফটওয়্যারটি ইনস্টল করা হয়। প্রতিটি শাখায় ল্যান ইনস্টল করা হয়েছিল এবং ভিসেট, রেডিও লিঙ্ক, ডিডিএন, ফাইবার অপটিক কেবল বা তাদের একটি সংমিশ্রণ ব্যবহার করে ল্যানগুলোকে ডেটা সেন্টারের সঙ্গে সংযুক্ত করা হয়। প্রতিটি শাখাকে সংযুক্ত করার জন্য দুটি রিডান্ডেন্ট লিঙ্ক ব্যবহার করা হতো।

সেন্ট্রালাইজড কোর ব্যাংকিং সিস্টেমে, গ্রাহকদের সমস্ত তথ্য এবং লেনদেনগুলো ডেটা সেন্টারে ক্লাস্টার সার্ভারগুলোর একটি গ্রুপের সঙ্গে সংযুক্ত একটি স্টোরেজ সিস্টেমে কেন্দ্রীয়ভাবে রেকর্ড করা হয়। ক্লাস্টারড সার্ভারগুলো সিস্টেমে রিডানডেন্সি প্রদান করে, এইভাবে একটি সার্ভার ব্যর্থ হলে, অন্য একটি সার্ভার সিস্টেমের নিয়ন্ত্রণ নেয় এবং সমস্ত শাখাকে সার্ভিস প্রদান করে। এই ধরনের সমাধানে, ডাটাবেসের একটি অনলাইন অনুলিপি বজায় রাখতে এবং সার্ভার এবং সরঞ্জামগুলোর একটি রিডানডেন্ট সেট রাখার জন্য একটি দূরবর্তী স্থানে ব্যাংকের একটি দুর্যোগ পুনরুদ্ধার সাইট (ডিআরএস) স্থাপন করতে হয়।

সেন্ট্রালাইজড কোর ব্যাংকিং সিস্টেমে, এটিএম/পিওএসের মতো অল্টারনেটিভ ডেলিভারি চ্যানেলগুলোকে সহজেই সংযোজন করা যেতে পারে, কারণ এটিএম/পিওএস সিস্টেম পৃথক শাখার সঙ্গে নয় বরং কেন্দ্রীয় সার্ভারের সঙ্গে সংযুক্ত থাকে। কেন্দ্রীয় সার্ভার, সরঞ্জাম এবং পরিবেশগুলো দিনে ২৪ ঘণ্টা, বছরে ৩৬৫ দিন চালানোর জন্য তৈরি করা হয়। বিশেষজ্ঞ আইটি পেশাদারদের ডেটা সেন্টারে পোস্টিং দেওয়া হয় এবং ডেটা সেন্টারের ২৪ ঘণ্টা পর্যবেক্ষণের জন্য রোস্টার ডিউটির ব্যবস্থা করা হয়।




*সেন্ট্রালাইজড ডাটাবেস সহ একটি ওয়্যান-ভিত্তিক কোর ব্যাংকিং সিস্টেম*

পরবর্তীতে, 'ওয়ান ব্যাংক' আই-ফ্লেক্স সলিউশন লিমিটেড, ইন্ডিয়ার 'মাইক্রোব্যাংকার' ব্যবহার করে; ব্র্যাক ব্যাংক এবং সিটি ব্যাংক ইনফোসিস লিমিটেড ইন্ডিয়ার 'ফিনাকল' ব্যবহার করে; প্রাইম ব্যাংক এবং এক্সিম ব্যাংক সুইজারল্যান্ডের গ্লোবাস প্রাইভেট লিমিটেড-এর টি২৪ ব্যবহার করে; এবি ব্যাংক এবং আইএফআইসি ব্যাংক মাইসিস পিএলসি, যুক্তরাজ্য-এর 'ইকোয়েশন' ব্যবহার করে এবং বেসিক ব্যাংক থ্রি-আই ইনফোটেক লিমিটেড, ভারতের 'ক্যাসেল কোর ব্যাংকিং' ব্যবহার করে কেন্দ্রীয় কোর ব্যাংকিং সিস্টেমে চালু করে।

ইতিমধ্যে, স্থানীয় সফটওয়্যার কোম্পানি যেমন ফ্লোরা সিস্টেমস, লিডস কর্পোরেশন, মিলেনিয়াম সফটওয়্যার এবং ইরা ইনফোটেক যথাক্রমে 'ফ্লোরা ব্যাংক অনলাইন', 'ব্যাংক আল্টিমাস', 'আবাবিল' এবং 'স্টিলার' নামে সেন্ট্রালাইজড কোর ব্যাংকিং সফটওয়্যার তৈরি করে।

বাকি ব্যাংকগুলো ২০০৭ সালের পর স্থানীয়ভাবে তৈরি ঐ সমস্ত সেন্ট্রালাইজড কোর ব্যাংকিং সফটওয়্যার ব্যবহার করা শুরু করে।

## ৫. ব্যাংক ও আর্থিক প্রতিষ্ঠানের জন্য বিভিন্ন সফটওয়্যার সিস্টেম

ব্যাংকগুলোতে, অনেক সফ্টওয়্যার বিভিন্ন উদ্দেশ্যে ব্যবহার করা হয়। আমানত এবং ঋণ গ্রাহকদের জন্য ব্যাংক অ্যাকাউন্ট খোলার জন্য এবং তাদের লেনদেন রেকর্ড করার জন্য ব্যবহৃত সফ্টওয়্যারকে কোর ব্যাংকিং সফটওয়্যার বলা হয়। এটিএম এবং পিওএস নেটওয়ার্ক পরিচালনার জন্য সুইচিং সফ্টওয়্যার প্রয়োজন। ক্রেডিট কার্ড ইস্যু এবং লেনদেন অনুমোদনের জন্য, ক্রেডিট কার্ড সফ্টওয়্যার ব্যবহার করা হয়। পেমেন্ট গেটওয়ে সফ্টওয়্যারটি ই-কমার্স লেনদেনের নিষ্পত্তির জন্য ব্যবহৃত হয়। মোবাইল ব্যাংকিং সফটওয়্যার মোবাইল অ্যাকাউন্ট খোলার জন্য এবং এই ধরনের লেনদেন রেকর্ড করার জন্য ব্যবহার করা হয়। ব্যাংকগুলো দ্বারা ব্যবহৃত প্রধান সফ্টওয়্যারগুলোর একটি সংক্ষিপ্ত বিবরণ নিচে দেওয়া হলো।

### ৫.১. কোর ব্যাংকিং সফটওয়্যার (Core banking software)

একটি ব্যাংকের মূল কার্যাবলির মধ্যে রয়েছে বিভিন্ন লেনদেনের একটি লেজার বজায় রাখা, গ্রাহকের তথ্য রাখা, ঋণ এবং আমানতের সুদের গণনা, অর্থ উত্তোলন ও জমার ক্ষেত্রে অ্যাকাউন্ট আপডেট করা ইত্যাদি। আগে এই কাজগুলো ম্যানুয়ালি করা হতো। আইসিটি (তথ্য ও যোগাযোগ প্রযুক্তি) এর আবির্ভাবের সঙ্গে, সফ্টওয়্যার অ্যাপ্লিকেশনগুলো ব্যবহার করে বিভিন্ন ব্যাংকিং প্রক্রিয়াকে স্বয়ংক্রিয় করা হয়—যাতে ব্যাংকিং কার্যক্রম পরিচালনা করা সহজ, দক্ষ এবং সাশ্রয়ী হয়। এভাবে, যে প্ল্যাটফর্মে আইসিটি ব্যবহার করে ব্যাংকের কার্যকলাপসমূহ সম্পাদন করা হয় তাহাকে কোর ব্যাংকিং সিস্টেম বলে এবং এই উদ্দেশ্যে ব্যবহৃত সফ্টওয়্যারটিকে কোর ব্যাংকিং সফ্টওয়্যার বলা হয়।

কোর ব্যাংকিং সিস্টেমে (সিবিএস), বিশাল ম্যানুয়াল লেজারের পরিবর্তে, ডিজিটাল আকারে ডেটা ব্যাকএন্ড ডেটাবেসে সংরক্ষণ করা হয়। একই সফ্টওয়্যার একটি ওয়্যান ব্যবহার করে একটি ব্যাংকের বিভিন্ন শাখায় ব্যবহার করা যেতে পারে। সুবিধা, একজন গ্রাহক ব্যাংকের যে কোনো শাখা থেকে তার অ্যাকাউন্ট পরিচালনা করতে পারেন এবং যদি ব্যাংকের ইন্টারনেট ব্যাংকিং বা এটিএম সুবিধা থাকে, তাহলে গ্রাহক কার্যত যে কোনো জায়গা থেকে তার অ্যাকাউন্ট পরিচালনা করতে পারেন।

সিবিএস উন্নত অপারেশনাল দক্ষতা নিশ্চিত করে এবং খরচ কমাতে সাহায্য করে। আন্তঃশাখা রিকনসিলিউশন দ্রুত এবং আরো সঠিক হয়।

এভাবে, কোর ব্যাংকিং সিস্টেম ব্যাংকগুলোর কাজ করার পদ্ধতিতে আমূল পরিবর্তন করেছে। একটি কোর ব্যাংকিং সিস্টেম থাকার সবচেয়ে বড় সুবিধা হলো যে নতুন প্রোডাক্ট প্রবর্তন কোন সময়সাপেক্ষ প্রক্রিয়া হয় না এবং আন্তঃশাখা ক্লিয়ারিং তাৎক্ষণিক সংঘটিত হয়ে যাবে। ব্যাংকগুলোর মধ্যে আন্তঃব্যাংক ইলেকট্রনিক তহবিল স্থানান্তর, স্টক মার্কেটে অনলাইন ট্রেডিং, ইত্যাদি সুবিধা প্রাক-কোর ব্যাংকিং সিস্টেম যুগে অজানা ছিল।

বর্তমানে বাজারে পাওয়া আন্তর্জাতিক কোর ব্যাংকিং অ্যাপ্লিকেশনগুলো হল টেমেনোস-এর টি ২৪, ওরাকল-এর ওরাকল ফিনান্সিয়াল সার্ভিসেস সফটওয়্যার (ওএফএসএস), এনফোসিস-এর ফিনাকল, মাইসিস-এর ইকোয়েশন, টাটা কনসালটালটেন্সি-এর টিসিএস ব্যাংক্স (TCS Bancs) এবং পোলারিস-এর এনটিলেক্ট স্যুট (Intellect Suite)।

স্থানীয়ভাবে প্রাপ্য কোর ব্যাংকিং সফ্টওয়্যার হলো ফ্লোরা সিস্টেমস লিমিটেডের 'ফ্লোরা ব্যাংক অনলাইন', লিডস কর্পোরেশনের 'ব্যাংক আল্টিমাস', মিলেনিয়াম সফটওয়্যারের 'আবাবিল' এবং ইরা ইনফোটেকের 'স্টিলার'।

### ৫.২. সুইচিং সফ্টওয়্যার (Switching software)

সুইচিং সফ্টওয়্যার হল একটি এটিএম/পিওএস লেনদেন প্রক্রিয়াকরণ এবং এদের ব্যবস্থাপনার উদ্দেশ্যে তৈরি একটি সিস্টেম যা নিম্নলিখিত উদ্দেশ্যে ব্যবহৃত হয়:

১. ডেবিট কার্ডের উৎপাদন এবং সঙ্গে সঙ্গে সিস্টেমে গ্রাহকের ডোঁ ঢোকানো ও তা ডাটাবেসে সংরক্ষণ করা।

২. অন-আস ডেবিট কার্ড লেনদেনের (ব্যাংকের নিজস্ব এটিএম/পিওএস-এ ব্যাংকের নিজস্ব কার্ডধারীদের দ্বারা করা লেনদেন) অথবা রিমোট অন-আস ডেবিট কার্ড লেনদেন (অন্য ব্যাংকের এটিএম/পিওএস-এ ব্যাংকের নিজস্ব কার্ডধারীদের দ্বারা করা লেনদেন) প্রাক-অনুমোদন করা। দ্রষ্টব্য : প্রাক-অনুমোদন বলতে কার্ড নম্বর, পিন, মেয়াদ শেষ হওয়ার তারিখ এবং কার্ডের বর্তমান অবস্থা (স্বাভাবিক, চুরি, হারিয়ে যাওয়া, ব্লক করা, হট-কার্ড ইত্যাদি) যাচাইকরণ বুঝায়।

৩. অন-আস বা রিমোট অন-আস লেনদেন নিজস্ব কোর ব্যাংকিং সিস্টেমে; অফ-আস (অন্য ব্যাংকের কার্ডধারী কর্তৃক আমাদের এটিএম/পিওএস-এ) লেনদেন ইস্যুকারী ব্যাংকের সুইচ বা ক্রেডিট কার্ড সিস্টেমে বা স্থানীয়/জাতীয় পেমেন্ট নেটওয়ার্কে (এনপিএসবি, কিউ-ক্যাশ, ক্যাশ লিঙ্ক, ইত্যাদি), অথবা আন্তর্জাতিক পেমেন্ট নেটওয়ার্কে (মাস্টারকার্ড, ভিসা, আমেরিকান এক্সপ্রেস, ডিনারস ক্লাব, ডিসকভার, ইত্যাদি) অগ্রিম অনুমোদনের জন্য পাঠানো।

৪. জালিয়াতি ব্যবস্থাপনা।

৫. সমস্ত সংযুক্ত এটিএম এবং পিওএস টার্মিনালের স্বাস্থ্য পর্যবেক্ষণ।

৬. সেটেলমেন্ট ও রিকনশিলিয়েশন।

স্ট্যান্ডার্ড সুইচিং সফ্টওয়্যার ওপেন সিস্টেম এবং ক্লায়েন্ট/সার্ভার বা ৩-স্তরের আর্কিটেকচার মেনে চলে। লেনদেন প্রক্রিয়াকরণ ইঞ্জিনটি শক্তিশালী ইউনিক্স প্ল্যাটফর্মে থাকে এবং ব্যবহারকারী ও এটিএম ডিভাইস ইন্টারফেসগুলো উইন্ডোজ ক্লায়েন্ট ওয়ার্কস্টেশনে থাকে। সিস্টেম ডেটা ওরাকলের মতো একটি ANSI কমপ্লায়েন্ট রিলেশনাল ডাটাবেসে সংরক্ষণ করা হয়।

একটি সাধারণ পরিবেশে, একটি সুইচিং সিস্টেম হোস্ট করা এটিএম/পিওএস টার্মিনাল থেকে কোর ব্যাংকিং সিস্টেম বা অন্য ব্যাংকের কোর ব্যাংকিং সিস্টেমে এবং আঞ্চলিক, জাতীয় বা আন্তর্জাতিক নেটওয়ার্কগুলোর সঙ্গে আইএসও ৮৫৮৩ ইন্টারফেস ব্যবহার করে সংযোগ প্রদান করে। পিন যাচাইকরণের জন্য হোস্ট সিকিউরিটি মডিউল (এইচএসএম), কার্ড উৎপাদনের জন্য একটি কার্ড আউটপুট ডিভাইস (বা কার্ড পার্সোনালাইজেশন সিস্টেম), কার্ডধারীদের এসএমএস পাঠানোর জন্য একটি স্বয়ংক্রিয় নোটিফিকেশন সিস্টেম এবং ক্রেডিট কার্ড ও কল সেন্টারের জন্য আনুষঙ্গিক অ্যাপ্লিকেশন ইত্যাদির সঙ্গেও সুইচিং সিস্টেমের ইন্টারফেস থাকে।

নিম্নলিখিত সুইচিং সফ্টওয়্যারগুলো বাংলাদেশের বিভিন্ন ব্যাংকে ব্যবহার করা হচ্ছে: এফআইএস গ্লোবাল সার্ভিসেস (ইউএসএ) এর আইএসটি/সুইচ, ইন্টার ব্লক (শ্রীলংকা)-এর আইসুইচ, টিয়েটো এনাটোর (লাটভিয়া) কার্ডস্যুট, টিপিএস (পাকিস্তান) এর ফনিক্স, ক্যাম্পাস প্লাস (রাশিয়া) এর ট্রান্সওয়্যার এবং ইউরোনেট (ইউএসএ) এর আইটিএম।

### ৫.৩. ক্রেডিট কার্ড সফটওয়্যার (Credit card software)

একটি ক্রেডিট কার্ড সফ্টওয়্যার হল ক্রেডিট কার্ড লেনদেন প্রক্রিয়াকরণ এবং ব্যবস্থাপনার জন্য ব্যবহৃত সিস্টেম, যা নিম্নলিখিত উদ্দেশ্যে ব্যবহৃত হয় :

১. ক্রেডিট কার্ডের উৎপাদন এবং সঙ্গে সঙ্গে সিস্টেমে গ্রাহকের ডেটা ঢোকানো ও তা ডেটাবেসে সংরক্ষণ করা।

২. অন-আস ক্রেডিট কার্ড লেনদেনের (ব্যাংকের নিজস্ব কার্ডহোল্ডারদের দ্বারা ব্যাংকের নিজস্ব এটিএম/পিওএস-এ করা লেনদেন) অথবা রিমোট অন-আস ক্রেডিট কার্ড লেনদেন (অন্যের এটিএম/পিওএস-এ ব্যাংকের নিজস্ব কার্ডধারীদের দ্বারা করা লেনদেনগুলো) প্রাক অনুমোদন করা। দ্রষ্টব্য : প্রাক-অনুমোদন বলতে কার্ড নম্বর, পিন, মেয়াদ শেষ হওয়ার তারিখ এবং কার্ডের বর্তমান অবস্থা (স্বাভাবিক, চুরি, হারিয়ে যাওয়া, ব্লক করা, হট কার্ড, ইত্যাদি) যাচাইকরণ এবং কার্ডের লিমিট ডেবিট করার পর লেনদেনের চূড়ান্ত অনুমোদন করাকে বুঝায়।

৩. অন-আস এবং রিমোট অন-আস ক্রেডিট কার্ড লেনদেনের অনুমোদন করা।

৪. অফ-আস (অন্য ব্যাংকের কার্ডধারী কর্তৃক আমাদের এটিএম/পিওএস-এ) লেনদেন অন্য ব্যাংকের ক্রেডিট কার্ড সিস্টেমে বা স্থানীয়/জাতীয় পেমেন্ট নেটওয়ার্কে (এনপিএসবি, কিউ-ক্যাশ, ক্যাশ লিংক ইত্যাদি), বা আন্তর্জাতিক পেমেন্ট নেটওয়ার্কে (মাস্টারকার্ড, ভিসা, আমেরিকান এক্সপ্রেস, ডিনারস ক্লাব, ডিসকভার ইত্যাদি) অগ্রিম অনুমোদনের জন্য পাঠানো।

৫. জালিয়াতি ব্যবস্থাপনা।

৬. সেটেলম্যান্ট ও রিকোনসিলিয়েশন।

নিম্নলিখিত ক্রেডিট কার্ড সফ্টওয়্যারগুলো বাংলাদেশের বিভিন্ন ব্যাংকে ব্যবহার করা হচ্ছে: টেইটো এনেটর (লাটভিয়া) এর ট্রান্সমাস্টার, সানগার্ড (ইউএসএ) এর কার্ড প্রো, ইন্টার ব্লকের (শ্রীলঙ্কা) আইকার্ড, কম্পাসের ট্রাঞ্জওয়্যার এবং কার্ড টেকের (সাইপ্রাস) সিটিএল প্রাইম।

### ৫.৪. পেমেন্ট গেটওয়ে সফটওয়্যার (Payment Gateway Software)

একটি পেমেন্ট গেটওয়ে সফ্টওয়্যার হলো একটি সফ্টওয়্যার, যা ই-কমার্স লেনদেনের অনুমোদন প্রদান করে থাকে। এটি খুচরা আউটলেটে অবস্থিত একটি পিওএস টার্মিনালের সমতুল্য। পেমেন্ট গেটওয়ের কিছু প্রধান বৈশিষ্ট্যের মধ্যে রয়েছে—

- সফ্টওয়্যার অ্যাপ্লিকেশনটি বিশেষত ই-কমার্সের জন্য ডিজাইন করা হয়েছে, যদিও এটি দোকান বা অফিসে পরিচালিত ব্যবসার লেনদেনের অনুমোদন করতেও ব্যবহার করা যেতে পারে।
- পেমেন্ট এবং ব্যক্তিগত তথ্য এনক্রিপশন করতে ব্যবহৃত হয়।
- সংশ্লিষ্ট আর্থিক প্রতিষ্ঠান, ব্যবসা এবং গ্রাহকের মধ্যে যোগাযোগ স্থাপন করে।
- পেমেন্টের অনুমোদন প্রদান করে থাকে।

কিছু পেমেন্ট গেটওয়েতে এমন টুল রয়েছে, যা গ্রাহকদের শিপিং এবং হ্যান্ডলিং খরচ, সেইসঙ্গে সেলস ট্যাক্স নির্ণয় করে তা আদায়ে সাহায্য করতে পারে। এছাড়াও জালিয়াতি শনাক্তকরণ টুল্স এবং অন্যান্য বৈশিষ্ট্য রয়েছে, যা পেমেন্ট গেটওয়ের সঙ্গে ব্যবহার করা হয়।

#### একটি পেমেন্ট গেটওয়ে সফ্টওয়্যারের কার্যাবলি

একটি পেমেন্ট গেটওয়ে সফ্টওয়্যার কার্ডধারীর তথ্য যথাক্রমে মার্চেন্ট পোর্টালে (যেমন একটি ওয়েবসাইট, মোবাইল ফোন বা আইভিআর সার্ভিস), অ্যাকোয়ারিং ব্যাংকে, পেমেন্ট অ্যাসোসিয়েশনে এবং সবশেষে কার্ড ইস্যুয়িং ব্যাংকে স্থানান্তর করতে সহায়তা করে। যখন একজন গ্রাহক পেমেন্ট গেটওয়ে-সক্ষম মার্চেন্টের কাছ থেকে একটি পণ্য অর্ডার করেন, তখন পেমেন্ট গেটওয়ে লেনদেন প্রক্রিয়াকরণের জন্য বিভিন্ন ধরনের কাজ করে থাকে, যেমন—

ক. যখন একজন গ্রাহক মার্চেন্টের ওয়েবসাইট থেকে কেনার জন্য কোন আইটেম নির্বাচন করেন এবং অর্থ প্রদানের জন্য 'চেকআউট' বা সমতুল্য বোতাম টিপেন, তখন ব্যাংকের পেমেন্ট গেটওয়ে সফ্টওয়্যারটি, যার সঙ্গে মার্চেন্টের ওয়েবসাইট লিঙ্ক করা হয়েছে তা সক্রিয় হয়ে যায় এবং গ্রাহক তার কার্ডের বিশদ বিবরণ সেখানে প্রবেশ করান।

খ. পেমেন্ট গেটওয়ে তারপর এসএসএল (সিকিউর সকেট লেয়ার) এনক্রিপশন ব্যবহার করে মার্চেন্টের ওয়েব সার্ভার থেকে লেনদেনের বিবরণ ব্যাংকের নিজস্ব সার্ভারে নিয়ে আসে।

গ. যদি লেনদেনটি একটি অন-আস কার্ড দ্বারা করা হয়, তাহলে পেমেন্ট গেটওয়ে লেনদেনের তথ্য ঐ ব্যাংকের কোর ব্যাংকিং সিস্টেমে (যদি ডেবিট কার্ড) বা ক্রেডিট কার্ড সিস্টেমে (যদি ক্রেডিট কার্ড হয়) পাঠায়।

ঘ. যদি কার্ডটি অফ-আস (বা নট অন-আস) হয়, পেমেন্ট গেটওয়ে কার্ড অ্যাসোসিয়েশনের (যেমন, ভিসা/মাস্টারকার্ড) কাছে লেনদেনের তথ্য পাঠায়।

ঙ. তারপর, কার্ড অ্যাসোসিয়েশন কার্ড ইস্যুকারী ব্যাংকের কাছে লেনদেন প্রক্রিয়া করার জন্য পাঠায়।

চ. কার্ড ইস্যুকারী ব্যাংক অনুমোদনের অনুরোধ গ্রহণ করে এবং কার্ড অ্যাসোসিয়েশনের মাধ্যমে পেমেন্ট গেটওয়েতে একটি রেসপন্স কোড ফেরত পাঠায়। পেমেন্টের ভাগ্য নির্ধারণের পাশাপাশি, (অর্থাৎ অনুমোদিত বা প্রত্যাখ্যানকৃত) লেনদেন ব্যর্থ হওয়ার কারণ (যেমন অপর্যাপ্ত তহবিল, বা ব্যাংকের লিঙ্ক পাওয়া যাচ্ছে না) নির্ধারণ করে তাহা রেসপন্স কোডের সঙ্গে প্রেরণ করে।

ছ. পেমেন্ট গেটওয়ে প্রতিক্রিয়াটি গ্রহণ করে এবং এটিকে মার্চেন্টের ওয়েবসাইটে (অথবা পেমেন্ট প্রক্রিয়া করার জন্য যে ইন্টারফেস ব্যবহার করা হয়েছিল তাহাতে) ফরোয়ার্ড করে। যেখানে এটিকে একটি সহজতম রেসপন্সে রূপান্তর করা হয় এবং তাহা কার্ডহোল্ডার এবং মার্চেন্টের কাছে ফেরত পাঠানো হয়।

জ. সম্পূর্ণ প্রক্রিয়াটি শেষ করতে সাধারণত ২-৩ সেকেন্ড সময় নেয়।

ঝ. মার্চেন্ট সেটেলমেন্টের উদ্দেশ্যে বিভিন্ন গ্রাহকদের দ্বারা সম্পন্ন করা লেনদেনের একটি 'ব্যাচ' কিছু সময় পর পর মার্চেন্ট 'বন্ধ' করে। ব্যাংক শুধু বন্ধ ব্যাচগুলোর জন্য দিনে এক বা একাধিকবার সেটেলমেন্ট করে থাকে।

ঞ. সেটেলমেন্টের সময়, পেমেন্ট গেটওয়ে মোট অনুমোদিত তহবিল চেক করে তা মার্চেন্টের অ্যাকাউন্টে জমা করে। মার্চেন্টের অ্যাকাউন্ট তার অ্যাকোয়ারিং ব্যাংকে বা অন্য কোনো ব্যাংকেও থাকতে পারে।

উপরের প্রক্রিয়ায়, সিরিয়াল নম্বর (ক) থেকে (ঘ), (ছ), এবং (ঝ) থেকে (ঞ) একটি পেমেন্ট গেটওয়ে সফ্টওয়্যারের কার্যাবলি বর্ণনা করে।

অনেক পেমেন্ট গেটওয়ে সফ্টওয়্যার প্রতারণার জন্য স্বয়ংক্রিয়ভাবে অর্ডার স্ক্রিন করে থাকে এবং অনুমোদনের জন্য অনুরোধ পাঠানোর আগে রিয়েল টাইমে ট্যাক্স গণনা করে থাকে। জালিয়াতি শনাক্ত করার টুলগুলোর মধ্যে রয়েছে ভূ-অবস্থান, ভেলোসিটি প্যাটার্ন বিশ্লেষণ, বিতরণ ঠিকানা যাচাইকরণ, কম্পিউটার ফিঙ্গারপ্রিন্টিং প্রযুক্তি, আইডেন্টিটি মরফিং শনাক্তকরণ এবং মৌলিক AVS (Address Verification System) চেক করা।

ভার্চুয়াল পেয়ার অথেনটিকেশন (ভিপিএ) হল অ্যাকোয়ারার, ইস্যুয়ারার এবং পেমেন্ট গেটওয়ের জন্য ক্রমবর্ধমান সাপোর্ট, যা ভিসার ৩-ডি সিকিউর, মাস্টারকার্ডের সিকিউরকোড এবং জেসিবি এর জে/সিকিউর হিসাবে পরিচিত। এসব অনলাইন পেমেন্টের নিরাপত্তার জন্য একটি অতিরিক্ত স্তর হিসাবে কাজ করে।

বাংলাদেশে, ডাচ-বাংলা ব্যাংক ৩রা জুন ২০১০-এ 'নেক্সাস গেটওয়ে' ব্র্যান্ড নামে দেশের প্রথম পেমেন্ট গেটওয়ে সফ্টওয়্যার চালু করে। 'কার্ড স্যুট ই-কমার্স' নামে সফ্টওয়্যারটি টিইটো এনাটর, লাটভিয়ার কাছ থেকে সংগ্রহ করা হয়েছে। নেক্সাস গেটওয়ে ডিবিবিএল-এর নেক্সাস কার্ড, মাস্টারকার্ড এবং ভিসা (বিশ্বের যেকোনো ব্যাংক দ্বারা ইস্যু করা) এর ডেবিট এবং ক্রেডিট কার্ড স্যুট গ্রহণ করে। এরপর ২০১০ সালের শেষের দিকে ব্র্যাক ব্যাংক তার ইন্টারনেট পেমেন্ট গেটওয়ে চালু করে। বর্তমানে অনেক ব্যাংক পেমেন্ট গেটওয়ে সার্ভিস চালু করেছে।

### ৫.৫. মোবাইল ফিন্যান্সিয়াল সার্ভিসের জন্য সফটওয়্যার

একটি মোবাইল ব্যাংকিং সফ্টওয়্যার বা মোবাইল ফিন্যান্সিয়াল সার্ভিসের জন্য সফ্টওয়্যার (এমএফএস) হলো একটি অ্যাপ্লিকেশন, যা একটি ব্যাংক মোবাইল ব্যবহারকারী, এজেন্ট এবং ব্যবসায়ীদের নিবন্ধন করতে ব্যবহার করে; ক্যাশ-ইন, ক্যাশ-আউট, পি২পি, পি২বি, বি২পি, পি২জি, জি২পি এবং এটিএম লেনদেন অনুমোদন এবং রেকর্ড করে।

পি২পি, পি২বি, বি২পি, পি২জি এবং জি২পি যথাক্রমে ব্যক্তি থেকে ব্যক্তি, ব্যক্তি থেকে ব্যবসা, ব্যবসা থেকে ব্যক্তি, ব্যক্তি থেকে সরকার এবং সরকার থেকে ব্যক্তিকে বোঝায়।

দেশের প্রথম এমএফএস ডাচ-বাংলা ব্যাংক 'রকেট' হিসাবে ৩১ মার্চ ২০১১ সালে চালু করেছিল এবং অল্প দিনের ব্যবধানে ব্র্যাক ব্যাংকের 'বিকাশ' আবির্ভূত হয়।

### ৫.৫.১. এমএফএস (MFS) বনাম কোর ব্যাংকিং সিস্টেম

একটি কোর ব্যাংকিং সিস্টেম এবং একটি এমএফএস এর মধ্যে নিম্নলিখিত প্রধান পার্থক্যগুলো হলো—

| আইটেম | কোর ব্যাংকিং সিস্টেম | এমএফএস সিস্টেম |
|---|---|---|
| হিসাব নাম্বার | প্রচলিত ব্যাংক অ্যাকাউন্ট নম্বর (একটি চেক ডিজিড সহ) | মোবাইল নম্বর + একটি চেক ডিজিড (ঐচ্ছিক) |
| গ্রাহক নিবন্ধন | শাখায় ব্যাংক অফিসার দ্বারা, বর্তমানে গ্রাহক ব্যাংকের অ্যাপ ব্যবহার করে ekyc-এর মাধ্যমে নিজে নিজেই অ্যাকাউন্ট খুলতে পারেন। | এজেন্ট দ্বারা মোবাইল নম্বর ইনপুট, ব্যাংক/তৃতীয় পক্ষ দ্বারা ডেটা এন্ট্রি, এবং ব্যাংক কর্তৃক কেওয়াইসি যাচাই করার পরে অনুমোদন। |
| যোগাযোগ | ওয়্যান (ফাইবার অপটিক, | মোবাইল নেটওয়ার্ক |

| | | |
|---|---|---|
| মাধ্যম/মিডিয়া | রেডিও লিঙ্ক, ভিসেট, ইত্যাদি) | (এসএমএস/ইউএসএসডি) এবং/অথবা ওয়্যান/ইন্টারনেট |
| পোস্টিং ডিভাইস | কম্পিউটার | মোবাইল ফোন এবং/অথবা কম্পিউটার |
| টাকা জমা | একটি শাখায় ব্যাংকের টেলার দ্বারা বা গ্রাহক নিজে ব্যাংকের CRM এ। | এজেন্ট দ্বারা |
| টাকা উত্তোলন | শাখায় ব্যাংকের টেলার দ্বারা অথবা গ্রাহক নিজেই ATM থেকে। | এজেন্ট থেকে অথবা এটিএম থেকে। |
| একটি নির্ধারিত সময়ে লেনদেনের সংখ্যা | সামান্য | বিপুল |
| প্রতি লেনদেনের পরিমাণ | বৃহৎ | ছোট |
| গ্রাহকের নাগাল | শাখার চারপাশে | সারা দেশে |

### ৫.৫.২. এমএফএস (MFS) বনাম এসএমএস (SMS) ব্যাংকিং সিস্টেম

মোবাইল ব্যাংকিং সিস্টেম একটি এসএমএস ব্যাংকিং সিস্টেম নয়। দুটি সিস্টেমের মধ্যে প্রধান পার্থক্য নিচে দেওয়া হলো–

| বিবরণ | এমএফএস | এসএমএস ব্যাংকিং সিস্টেম |
|---|---|---|
| গ্রাহকদের অ্যাক্সেস: | মোবাইল ওয়ালেট/ মোবাইল একাউন্ট | ব্যাংক অ্যাকাউন্ট (সঞ্চয়ী, সিডি, এসএনডি, ইত্যাদি) |
| নগদ লেনদেন | ব্যাংকের শাখা, এটিএম বা এজেন্ট পয়েন্টে | নগদ লেনদেন করা যায় না |
| সিস্টেম অ্যাক্সেস করতে গ্রাহকের দ্বারা ব্যবহৃত ডিভাইস: | মোবাইল সেট বা এটিএম | শুধু মোবাইল সেট |
| গ্রাহক এবং ব্যাংকের মধ্যে সংযোগ | এসএমএস, ইউএসএসডি, ইডটিকে, এসটিকে বা BREW | শুধু এসএমএস |
| মার্চেন্ট পেমেন্ট | সম্ভব | সম্ভব নয় |
| ইউটিলিটি বিল প্রদান | সম্ভব | সম্ভব |

দ্রষ্টব্য: এসএমএস মানে সর্ট মেসেজিং সিস্টেম, ইউএসএসডি মানে Unstructured Supplimentary Service Data, ইউআইএম মানে User Identity Management, এসটিকে মানে Sim Tool Kit এবং BREW হলো Binary Runtime Environment for Wireless.

### ৫.৫.৩. মোবাইল ফাইন্যান্সিয়াল সার্ভিসের (এমএফএস) জন্য সহজলভ্য সফ্টওয়্যার

বাংলাদেশে, ডাচ-বাংলা ব্যাংক, সাইবেস মবিলাইজার নামে সফ্টওয়্যার ব্যবহার করে ৩১ মার্চ ২০১১ সালে প্রথমবারের মতো মোবাইল ফাইন্যান্সিয়াল সার্ভিস বা এমএফএস শুরু করে। ব্র্যাক ব্যাংক ফান্ডামো-কে তাদের এমএফএস প্ল্যাটফর্ম হিসেবে বেছে নিয়েছে। বাণিজ্যিকভাবে পাওয়া যায় এমন এমএফএস সফ্টওয়্যার নিচে তালিকাভুক্ত করা হয়েছে—

| সফটওয়্যারটির নাম | ডেভেলপার |
|---|---|
| ১. রকেট | ডাচ-বাংলা ব্যাংক |
| ২. সাইবেস মবিলাইজার | সাইবেজ ৩৬৫, জার্মানি (এখন, SAP, ইউএসএ দ্বারা ক্রয়কৃত) |
| ৩. কমভিভা | কমভিভা টেকনোলজিস লিমিটেড, ভারত |
| ৪. এম-চেক | এমচেক লিমিটেড, ভারত |
| ৫. ফান্ডামো | ফান্ডামো লিমিটেড, দক্ষিণ আফ্রিকা |
| ৬. ওবোপে | ওবোপে, ইউএসএ |
| ৭. বিকাশ | হুয়াওয়ে ফিনটেক সলিউশন |
| ৮. নগদ ডিএফএস | কনা সফটওয়্যার ল্যাব, কোরিয়া |

### ৫.৫.৪. এমএফএসের গ্রাহক এবং তাদের জন্য মেনু আইটেম

মোবাইল ব্যাংকিংয়ে তিন ধরনের গ্রাহক জড়িত। তারা হলো ভোক্তা, এজেন্ট এবং মার্চেন্ট।

**ভোক্তা (Consumer)**

ভোক্তা হলেন মোবাইল ফোনের মালিক, যিনি এমএফএস জন্য নিবন্ধিত। তাদের মোবাইল ডিভাইসে, তারা সাধারণত নিম্নলিখিত মেনু পাবেন—

- ব্যালেন্স চেক করা।
- মিনি স্টেটমেন্ট।
- তহবিল স্থানান্তর (পিটুপি)।
- ইউটিলিটি বিল পেমেন্ট।
- টিউশন ফি প্রদান।
- মোবাইল টপআপ।
- পিন পরিবর্তন করা, ইত্যাদি।

**এজেন্ট**

এজেন্টরা হলো ব্যাংক-মনোনীত কোনো দোকানের মালিক যারা ব্যাংকের হয়ে গ্রাহক নিবন্ধন এবং নগদ লেনদেন করেন। তাদের মোবাইল ডিভাইসে, তারা সাধারণত নিম্নলিখিত মেনু পাবেন—

- গ্রাহক নিবন্ধন করা।
- ক্যাশ-ইন।
- ক্যাশ-আউট, ইত্যাদি।

**মার্চেন্ট**

মার্চেন্ট হলো ব্যাংক-মনোনীত কিছু দোকানের মালিক, যারা তাদের পণ্য ও পরিষেবা বিক্রি করার পর গ্রাহকদের মোবাইল ওয়ালেট থেকে তাদের নিজস্ব মোবাইল ওয়ালেটে অর্থ সংগ্রহ করে। তাদের মোবাইল ডিভাইসে, তারা সাধারণত নিম্নলিখিত মেনু পাবেন—

- মার্চেন্ট পেমেন্ট।
- ব্যালেন্স চেক।
- মিনি স্টেটম্যান্ট, ইত্যাদি।

**৫.৫.৫. মোবাইল ফাইন্যান্সিয়াল সার্ভিসের (এমএফএস) জন্য সফটওয়্যারের বৈশিষ্ট্য**

একটি মোবাইল ব্যাংকিং সফ্টওয়্যারের নিম্নলিখিত বৈশিষ্ট্য থাকা উচিত—

- এসএমএস, ইউএসএসডি, ইউটিকে, এসটিকে, বা বিআরইডাব্লুউ ব্যবহার করে মোবাইল অপারেটরের মাধ্যমে মোবাইল ব্যবহারকারী, এজেন্ট এবং ব্যবসায়ীদের সঙ্গে সংযোগ প্রদান করা। এসএমএস-এর অর্থ হলো শর্ট মেসেজিং সিস্টেম, ইউএসএসডি-এর অর্থ Unstructured Supplementary Service Data, এসটিকে হলো Sim Tool Kit এবং বিআরইডাব্লিউ হলো Binary Runtime Environment for Wireless. এজেন্ট, ভোক্তা, বা মার্চেন্টের দ্বারা নিম্নলিখিত কাজগুলো সম্পাদন করার সুবিধা প্রদান করে—
- ভোক্তা, এজেন্ট, এবং মার্চেন্ট রেজিস্ট্রেশন করা
- নগদ: এজেন্ট, ব্যাংক শাখা এবং এটিএম-এর মাধ্যমে ক্যাশ-ইন/ক্যাশ-আউট করা
- পি২পি: একজন গ্রাহকের মোবাইল অ্যাকাউন্ট থেকে অন্য গ্রাহকের মোবাইল অ্যাকাউন্টে তহবিল স্থানান্তর
- পি২বি: ইউটিলিটি বিল পেমেন্ট, টিউশন ফি পেমেন্ট, মোবাইল টপআপ, মার্চেন্ট পেমেন্ট, বাস/রেলওয়ে/এয়ারলাইন টিকিট কেনা, সিনেমার টিকিট ক্রয়
- বি২পি : কর্পোরেট সংস্থা / শিল্প সংস্থা/ অফিস কর্তৃক বেতন বিতরণ এবং বৈদেশিক রেমিট্যান্স প্রদান
- জি২পি : সরকারি বয়স্ক ভাতা, মুক্তিযোদ্ধা ভাতা, ইত্যাদি বিতরণ।

**অন্যান্য বৈশিষ্ট্য**

- অডিট ট্রেইল।
- মেকার এন্ড চেকার।
- যদি ইন্টারফেসটি ইউএসএসডি, ইউটিকে, এসটিকে বা বিআরইডাব্লুউ হয় তাহলে পিন যাচাইকরন
- ইন্টারফেসটি যদি এসএমএস হয়, তাহলে আইভিআরের মাধ্যমে পিন যাচাই করা।
- কিছু মোবাইল নেটওয়ার্ক অপারেটর (এমএনও) এর জন্য এসএমএস এবং অন্য কিছু এমএনও-এর জন্য ইউএসএসডি, ইউটিকে, এসটিকে, বা বিআরইডাব্লিউ ব্যবহার করা।
- সমস্ত লেনদেনের জন্য গ্রাহককে এসএমএস-এর মাধ্যমে একটি নিশ্চিতকরণ বার্তা পাঠানো।
- ব্যাংক, এজেন্ট এবং এমএনও-এর মতো পক্ষগুলোর মধ্যে আয়ের ভাগাভাগি।
- মার্চেন্টের পেমেন্ট দেওয়ার সময় কমিশন কর্তন করা এবং তা ব্যাংক ও এমএনও এর মধ্যে ভাগাভাগি করা।
- মাসের শেষে ভ্যাট কর্তন।

- বিভিন্ন পরিষেবার জন্য ফি এবং চার্জ সেট আপ করা।
- ডিপোজিট একাউন্টে সুদ নির্ণয়।
- এজেন্টদের ক্রেডিট সুবিধা প্রদান এবং তার জন্য সুদ নির্ণয় করা
- ডে-এন্ড প্রক্রিয়া করা।

## ৫.৬. এজেন্ট ব্যাংকিং এর জন্য সফটওয়্যার

### ৫.৬.১. এজেন্ট ব্যাংকিং সিস্টেমের জন্য সফটওয়্যার

এজেন্ট ব্যাংকিং হলো বায়োমেট্রিকভিত্তিক ব্যাংকিং সফ্টওয়্যার যেখানে, সমস্ত লেনদেন আঙুলের ছাপ প্রমাণীকরণের মাধ্যমে যাচাই করা হয়। এজেন্ট ব্যাংকিংয়ের গ্রাহকদের সব কোর ব্যাংকিং সিস্টেম সুবিধা প্রদান করা হয়। প্রত্যন্ত অঞ্চলে ব্যাংকিং সুবিধা ছড়িয়ে দেওয়ার জন্য যেখানে প্রচলিত ব্যাংকিং সেবা চালু নেই, সেই গ্রাহকদের লক্ষ্য করে এজেন্ট ব্যাংকিং চালু করা হয়েছিল।
এজেন্ট ব্যাংকিং সফ্টওয়্যার হলো একটি অ্যাপ্লিকেশন, যা ব্যাংকগুলো গ্রাহক, এজেন্ট এবং মার্চেন্টদের অ্যাকাউন্ট খুলতে ব্যবহার করে; ক্যাশ-ইন, ক্যাশ-আউট, ফান্ড ট্রান্সফার, বিল পেমেন্ট, বেতন বিতরণ, এটিএম উত্তোলন এবং ইকমার্স লেনদেন অনুমোদন ও রেকর্ড করুন।

এই সফ্টওয়্যারের মাধ্যমে, প্রায় সমস্ত পরিষেবা প্রধানত ব্যাংক-মনোনীত এজেন্ট আউটলেটগুলো দ্বারা সরবরাহ করা হয়। এজেন্ট ব্যাংকিং গ্রাহকরা ব্যাংক শাখা থেকেও নির্দিষ্ট সেবা পেতে পারেন।

### ৫.৬.২. এজেন্ট ব্যাংকিং সিস্টেম বনাম কোর ব্যাংকিং সিস্টেম

একটি কোর ব্যাংকিং সিস্টেম এবং একটি এজেন্ট ব্যাংকিং সিস্টেমের মধ্যে প্রধান পার্থক্যগুলো হলো—

| আইটেম | এজেন্ট ব্যাংকিং সিস্টেম | কোর ব্যাংকিং সিস্টেম |
|---|---|---|
| হিসাব নাম্বার | প্রচলিত ব্যাংক অ্যাকাউন্ট নম্বর (একটি চেক ডিজিট সহ) | প্রচলিত ব্যাংক অ্যাকাউন্ট নম্বর (একটি চেক ডিজিটসহ) |
| গ্রাহক নিবন্ধন | • পিওএস ডিভাইস/ডেস্কটপ অ্যাপ্লিকেশনের মাধ্যমে এজেন্টগণ গ্রাহকের ফ্রিঙ্গার প্রিন্ট গ্রহণ করেন। | শাখায় ব্যাংক অফিসার দ্বারা |
| | • এজেন্ট/টেলার গ্রাহকদের কেওয়াইসি-এন্ট্রি করে<br>• ব্যাংক কর্মকর্তা কেওয়াইসি যাচাই করার পর গ্রাহক নিবন্ধন অনুমোদন করেন। | |
| যোগাযোগ মাধ্যম | • পিওএস-এর জন্য : সুরক্ষিত মোবাইল ডেটা ব্যবহার করা হয়।<br>• ডেস্কটপ অ্যাপের জন্য : ভিপিএন দ্বারা সুরক্ষিত ইন্টারনেট নেটওয়ার্ক ব্যবহার করা হয়। | ওয়্যান (ফাইবার অপটিক, রেডিও লিঙ্ক, ভিসেট ইত্যাদি) ব্যবহার করা হয়। |
| পোস্টিং ডিভাইস | • বায়োমেট্রিক POS<br>• পিসি/ল্যাপটপ | কম্পিউটার |
| টাকা জমা করা | • শাখায় ব্যাংকের টেলার দ্বারা<br>• এজেন্ট আউটলেটে | • শাখায় ব্যাংকের টেলার দ্বারা |
| টাকা উত্তোলন | • শাখায় ব্যাংকের টেলার দ্বারা<br>• এজেন্ট আউটলেটে<br>• ATM -এ | • শাখায় ব্যাংকের টেলার দ্বারা<br>• এটিএম-এ |
| একটি নির্দিষ্ট সময়ে লেনদেনের সংখ্যা | অনেক | কয়েকটি |
| প্রতি লেনদেনের পরিমাণ | মাধ্যম | প্রচুর পরিমাণ |
| গ্রাহকের নাগাল | সারা দেশে | শাখার চারপাশে |

### ৫.৬.৩. এজেন্ট ব্যাংকিং সিস্টেম বনাম এমএফএস (MFS)

| আইটেম | এজেন্ট ব্যাংকিং সিস্টেম | এমএফএস |
|---|---|---|
| হিসাব নাম্বার | প্রচলিত ব্যাংক অ্যাকাউন্ট নম্বর (চেক ডিজিটসহ) | মোবাইল নম্বর |
| গ্রাহক নিবন্ধন | • অ্যাপ্লিকেশন ব্যবহার করে এজেন্টগণ গ্রাহকের ফিঙ্গার প্রিন্ট গ্রহণ করেন।<br>• এজেন্ট/টেলার গ্রাহকের কেওয়াইসি এন্ট্রি করেন।<br>• ব্যাংক কর্মকর্তা কেওয়াইসি যাচাই করার পর গ্রাহক নিবন্ধন অনুমোদন করেন। | • এজেন্ট দ্বারা মোবাইল নম্বর ইনপুট করা হয়।<br>• ব্যাংক/তৃতীয় পক্ষ দ্বারা ডেটা এন্ট্রি করা হয়।<br>• কেওয়াইসি যাচাই করার পরে ব্যাংক অফিসার দ্বারা অনুমোদন করা হয়। |
| যোগাযোগের মাধ্যম | • পিওএস এর জন্য : সুরক্ষিত মোবাইল ডেটা ব্যবহার করা হয়।<br>• ডেস্কটপ অ্যাপের জন্য : ভিপিএন দ্বারা সুরক্ষিত, ইন্টারনেট নেটওয়ার্ক ব্যবহার করা হয়। | মোবাইল নেটওয়ার্ক (এসএমএস/ইউএসএসডি) এবং/অথবা ওয়্যান/ইন্টারনেট |
| পোস্টিং ডিভাইস | • বায়োমেট্রিক POS<br>• পিসি/ল্যাপটপ | মোবাইল ফোন এবং/অথবা কম্পিউটার |
| টাকা জমা করা | • শাখায় ব্যাংকের টেলার দ্বারা।<br>• এজেন্ট আউটলেটে। | • শাখায় ব্যাংকের টেলার দ্বারা।<br>• এজেন্ট আউটলেটে। |
| টাকা উত্তোলন | • শাখায় ব্যাংকের টেলার দ্বারা।<br>• এজেন্ট আউটলেটে। | • শাখায় ব্যাংকের টেলার দ্বারা।<br>• এজেন্ট আউটলেটে।<br>• এটিএম-এ। |
| একটি নির্দিষ্ট সময়ে লেনদেনের সংখ্যা | অনেক | বিপুল |
| প্রতি লেনদেনের পরিমাণ | মধ্যম | সামান্য |
| গ্রাহকের নাগাল | সারা দেশ | সারা দেশ |

### ৫.৬.৪. এজেন্ট ব্যাংকিং সিস্টেম-এ ব্যবহৃত ডিভাইসের প্রকার

এজেন্ট ব্যাংকিং সফ্টওয়্যারের মূল হলো বায়োমেট্রিক প্রমাণীকরণ মডিউল। কারণ আঙুলের ছাপের মাধ্যমে লেনদেনগুলোর বৈধতা সম্পন্ন করা হয়। প্রমাণীকরণের উদ্দেশ্যে, লেনদেনের প্রকারের ভেদে গ্রাহক এবং এজেন্টদের আঙুলের ছাপ ক্যাপচার করতে বিভিন্ন ধরনের ডিভাইস ব্যবহার করা হয়।

| ডিভাইস | বিবরণ | উৎপাদনকারী প্রতিষ্ঠান |
|---|---|---|
| বায়োমেট্রিক পিওএস | এটি একটি ইন-বিল্ট ফিঙ্গারপ্রিন্ট স্ক্যানার মডিউলসহ একটি পিওএস ডিভাইস। যাকে বায়োমেট্রিক পিওএস বলা হয়। | ✓ ভেরিফোন<br>✓ ইন্‌জেনিকো<br>✓ FAX |
| ফিঙ্গারপ্রিন্ট স্ক্যানার | ফিঙ্গারপ্রিন্ট ক্যাপচার করার জন্য কম্পিউটারের সঙ্গে ফিঙ্গারপ্রিন্ট স্কেনার ডিভাইস ব্যবহার করা হয়। | ✓ সেকুজেন<br>✓ অ্যাবেট্রি<br>✓ মরফো<br>✓ ডার্মালগ |

### ৫.৬.৫. নিরাপত্তা (Security)

নেটওয়ার্ক ও ব্যাংকিং সিস্টেমের জন্য সিস্টেম-সম্পর্কিত নিরাপত্তার পাশাপাশি, এজেন্ট ব্যাংকিং সফ্টওয়্যার কিছু অ্যাপ্লিকেশন স্তরের নিরাপত্তা নিশ্চিত করে।

| | |
|---|---|
| বায়োমেট্রিক পিওএস ডিভাইস | • নিবন্ধিত ডিভাইসগুলো নির্দিষ্ট ব্যবহারকারীদের সঙ্গে বাইন্ডেড থাকে, যাতে অন্য কেউ সেই ডিভাইসটি |

| | |
|---|---|
| | অ্যাক্সেস করতে না পারে।<br>• সমস্ত অনুরোধ এবং রেসপন্স এনক্রিপ্ট করে প্রেরণ করা হয়। |
| ডেস্কটপ অ্যাপ্লিকেশন | • নতুন ডিভাইস রেজিস্ট্রেশনের অনুরোধগুলো এজেন্ট দ্বারা পিন প্রমাণীকরণ এবং নিবন্ধিত মোবাইল ফোনে ওটিপি পাঠায়ে শুরু করা হয়।<br>• ব্যাংক অ্যাডমিনকে নতুন যোগ করা ডিভাইসগুলোকে অনুমোদন করতে হয়, যাতে এজেন্ট তা ব্যবহার করতে পারে।<br>• অনুমোদনের পর ম্যাপ করা ব্যবহারকারীদের দ্বারা শুধু নিবন্ধিত ডিভাইসগুলো অ্যাক্সেস করা যাবে।<br>• সমস্ত অনুরোধ এবং রেসপন্স এনক্রিপশনসহ প্রেরণ করা হয়।<br>• জেন্ট লগইন করার সময় আরএসএ প্রমাণীকরণ প্রয়োজন হয়। |

### ৫.৬.৬ এজেন্ট ব্যাংকিং সিস্টেমের জন্য প্রাপ্ত সফ্টওয়্যার

বিভিন্ন সফটওয়্যার কোম্পানি এজেন্ট ব্যাংকিং সফ্টওয়্যার তৈরি করে। যেহেতু এজেন্ট ব্যাংকিং সিস্টেম কোর ব্যাংকিং সিস্টেমের মতোন সেবা প্রদান করে, তাই অনেক কোর ব্যাংকিং সিস্টেম ডেভেলপার এজেন্ট ব্যাংকিংয়ের জন্য সফ্টওয়্যার তৈরি করে।

| সফটওয়্যারের নাম | ক্লায়েন্ট |
|---|---|
| ডিবিবিএল এজেন্ট ব্যাংকিং সফটওয়্যার (ইন-হাউস) | ডাচ্-বাংলা ব্যাংক |
| এজেন্ট ব্যাংকিং সিস্টেম, ইরা-ইনফোটেক | • ব্যাংক এশিয়া<br>• ইউনাইটেড কমার্শিয়াল ব্যাংক<br>• শাহজালাল ইসলামী ব্যাংক এনআরবি ব্যাংক<br>• প্রাইম ব্যাংক<br>• সাউথইস্ট ব্যাংক<br>• সিটি ব্যাংক<br>• যমুনা ব্যাংক<br>• সোনালী ব্যাংক |
| ইন্টিগ্রেটেড এজেন্ট ব্যাংকিং সলিউশন (আইএবিএস)<br><br>ইসলামী ব্যাংক (ইন-হাউস) | ইসলামী ব্যাংক |
| মিলেনিয়াম ইনফরমেশন সলিউশন, বাংলাদেশ | আল-আরাফাহ ইসলামী ব্যাংক<br>সোস্যাল ইসলামিক ব্যাংক লিঃ |
| **এম**-ফিনো, ভারত | ব্র্যাক ব্যাংক |
| সেলোস্কোপ, বাংলাদেশ | এনআরবিসি ব্যাংক<br>অগ্রণী ব্যাংক |
| ইজি ব্যাংক (ইন-হাউস) | ইস্টার্ন ব্যাংক |
| মাইক্রো সলিউশন, বাংলাদেশ | মার্কেন্টাইল ব্যাংক |
| ফ্লোরা এজেন্ট ব্যাংকিং সিস্টেম<br>ফ্লোরা সিস্টেমস, বাংলাদেশ | মিডল্যান্ড ব্যাংক<br>ওয়ান ব্যাংক<br>সাউথ বাংলা এগ্রিকালচার অ্যান্ড কমার্স ব্যাংক |
| মধুমতি ডিজিটাল ব্যাংকিং<br>ডেটাসফট, বাংলাদেশ | মধুমতি ব্যাংক |
| **এনকোর**, লিডস কর্পোরেশন | প্রিমিয়ার ব্যাংক |

### ৫.৬.৭. এজেন্ট ব্যাংকিংয়ের গ্রাহক এবং তাদের জন্য মেনু আইটেম

এজেন্ট ব্যাংকিংয়ে প্রধানত দুই ধরনের গ্রাহক জড়িত। তারা ভোক্তা এবং এজেন্ট।

**ভোক্তা :** যদি ব্যাংক কোনো গ্রাহকদের জন্য অ্যাপ্লিকেশন যেমন মোবাইল অ্যাপস, ইন্টারনেট ব্যাংকিং ইত্যাদি তৈরি না করে, তবে গ্রাহকরা সরাসরি এজেন্ট ব্যাংকিং সিস্টেমে অ্যাক্সেস করতে পারবেন না। তাই তাদের জন্য কোনো মেনু প্রযোজ্য নয়।

**এজেন্ট :** ব্যাংক-মনোনীত এজেন্টরা হলো প্রধান লেনদেনের সূচনাকারী যারা ব্যাংকের পক্ষে গ্রাহক নিবন্ধন এবং নগদ লেনদেন সম্পাদন করবে। তাদের বায়োমেট্রিক পিওএস বা ডেস্কটপ অ্যাপ্লিকেশনে, তারা নিম্নলিখিত মেনু পাবেন :

- গ্রাহক নিবন্ধন।
- ক্যাশ-ইন।
- ক্যাশ-আউট।
- তহবিল স্থানান্তর।
- বিল পেমেন্ট।
- চেক ব্যালেন্স।
- চেক স্টেটমেন্ট।

**৫.৬.৮. এজেন্ট ব্যাংকিং সেবার জন্য ব্যবহৃত একটি সফ্টওয়্যারের বৈশিষ্ট্য**

**রেজিস্ট্রেশন প্রক্রিয়া**

- সুপার-এজেন্ট, এজেন্ট, ডিএসআর, সাব-এজেন্ট, ফাস্ট-ট্র্যাক অফিসার, RO এবং টেলারের নিবন্ধন করার মডিউল ।
- নতুন গ্রাহকদের নিবন্ধন।
- কোর ব্যাংকিং গ্রাহকদের লিঙ্কিং।
- বিল গ্রহণকারীর নিবন্ধন।
- আঙুলের ছাপের পরিবর্তন।
- এজেন্ট/সাব-এজেন্টের প্রতিস্থাপন।
- এজেন্ট শ্রেণিবিন্যাস ব্যবস্থাপনা।

**সেবাসমূহ**

- ক্যাশ-ইন এবং ক্যাশ-আউট।
- ইউটিলিটি বিল পেমেন্ট।
- ব্যালেন্স এবং স্টেটমেন্ট চেক করা।
- তহবিল স্থানান্তর।
- এটিএম লেনদেন।
- POS এবং ই-কমার্স লেনদেন।
- বেতন আপলোড।
- ঋণ বিতরণ।
- বিভিন্ন শ্রেণির এজেন্ট কর্তৃক তহবিল ব্যবস্থাপনা।
- এজেন্ট পয়েন্ট এবং শাখার মাধ্যমে রেমিট্যান্স বিতরণ।

**অন্যান্য অপারেশন বা কার্যাবলি**

- সমস্ত লেনদেনের জন্য গ্রাহককে এসএমএসের মাধ্যমে একটি নিশ্চিতকরণ বার্তা পাঠাতে হবে।
- ডে এন্ড প্রক্রিয়া।
- বিভিন্ন শ্রেণির এজেন্টদের মধ্যে কমিশন বিতরণ।
- এজেন্ট ও সাব এজেন্টকে তাদের ডিপোজিটের ওপর কমিশন প্রদান।
- সার্ভিস চার্জ, সুদ এবং লেনদেনের সীমা নির্ধারণ।
- সিস্টেম দ্বারা মাসের শেষে ভ্যাট কর্তন।
- বিভিন্ন পরিষেবার জন্য ফি এবং চার্জ নির্ণয়।
- আমানত অ্যাকাউন্টে সুদের হিসাব করা।
- বিভিন্ন পক্ষের মধ্যে আয় ভাগাভাগি যেমন ব্যাংক, এজেন্ট ইত্যাদি।

# পর্যালোচনামূলক প্রশ্নাবলি

## 1. Multiple Choice Questions (MCQ)

i) Recommended temperature for a Data Center is ….. degree C and humidity is ….. %

a) 10, 38 b) 20, 70 c) 25, 50 d) 20, 50

ii) Higher data transfer rate is found in …..

a) LAN b) Internet c) WAN d) VSA

iii) A router is used in …..

a) LAN b) Internet c) WAN d) Hard Disk

iv) A VSAT is used in …..

a) LAN b) Internet c) WAN d) Router

v) The largest WAN is …..

a) ICT Ministry Network b) Facebook network c) Internet d) SWIFT

vi) The most popular implementation of RAID is level …..

a) Level-5 b) Level 0 c) Level 1 d) Level 0+1

vii) Which of the following is not a part of LAN?

a) Router b) Network Switch c) LAN d) Computer

viii) Which of the following is not a transmission media of LAN?

a) Coaxial Cable b) Wi-fi c) Fiber Optic Cable d) VSAT

ix) Which of the following is the transmission media of WAN?

a) Microwave b) Wi-fi c) Coaxial Cable d) Twisted-Pair Cable

x) Firewall is used in a WAN for which of the following?

a) Additional Bandwidth b) Additional Security c) Additional distance d) Additional Accuracy

xii) Where a Dark Fiber is used?

a) Between DC and DRS. b) In a wi-fi . c) Between LAN and WAN d) In computer programming

xiii) Why a SAN switch is used?

a) To connect Servers with a Storage. b) To connect WAN and LAN. c) To connect two cities. d) To connect two bank branches

## 2. Fill in the Gap(s)

i) The run length of individual Ethernet Cables in LAN is limited to roughly ….. meters.

ii) LAN follows either …… or …..architecture?

iii) For setup of an ICT infrastructure of a bank having 50 branches, the approximate budget requirement is Taka …..million.

iv) In the LAN-based approach of bank automation, …..or Novel operating systems was used. The data was stored in a server as flat file or database either …..or dBase. The application software was written in…..or dBase.

v) Nexus Gateway was lunched for the first time in Bangladesh by Dutch-Bangla Bank in the year of ……

vi) Rocket was the first MFS in Bangladesh launched by Dutch-Bangla Bank on …..

vii) Near Data Center is a Data Center established in the same city where …..is located.

viii)The DRS should have capability to become primary site automatically in case the ….. is in disaster.

ix) One of the common data center certification awarded by the ‘Uptime Institue’ is ….. certification.

x) A WAN connects two or more …..

xi) The largest WAN in existence is …..

x) Bandwidth of a VSAT is ….. than that of Radio Link.

xi) DMZ in Computer Networking stands for …..

xii) In the 3-tier architecture of computer programming technique, normally user's computer termials, application server and…..are involved.

xiii) P2G stands for…..

## সম্ভাব্য প্রশ্নাবলি

1. What is a Data Center? What are the basic requirements of a Tier-4 Data Center?
2. Why near Data Center is important for FIs?
3. Why FIs setup DRS? What points need to be considered during selection of distance between a DC and a DRS?
4. Narrate advantage and disadvantages of Tier-1, Tier-2, Tier-3 and Tier-4 data centers.
5. What is LAN card? Why it is needed in a LAN?
6. Name 3 LAN and 3 WAN communication media.
7. Mention a few of the differences between LAN andWAN?
8. Describe advantages and disadvantages between the following data transmission media for a WAN of a Bank: Land Line, Microwave and Satellites.
9. Why Firewall is installed in the networking system of a bank?
10. Why DMZ needed to be established in the network system of a bank?
11. Narrate functions of a branch server, application server and database server.
12. What is the 3-tier architecture of computer programming?
13. What is RAID? Why RAID is used in Banking system?
14. What are the differences between a RAID level 0 and 1? What do you mean by RAID level 0+1?
15. What do you mean by computer clustering? Why clustering is used in a computer system of a bank?
16. Define replication with an example.

17. What is dark fiber cable and where is used in a banking system?
18. Why a banking system uses external storage instead of an internal storage for storage of its data?
19. Define SAN switch.
20. Why database backup is important in banking?
21. What are the three types database backup? Explain each of them. Which one is suitable for your bank/FI?
22. What do you mean by Alternative Delivery Channel?
23. Mention some disadvantages of a stand alone approach of bank automation.
24. Narrate history of online banking in Bangladesh.
25. Mention 3 functions of each of the following software: a) Core Banking Software, b) Switching Software, c) Credit Card Software, d) Payment Gateway Software.
26. Why each of the following software are used in Banks? - a) Core Banking Software, b) Switching Software, c) Credit Card Software, d) Payment Gateway Software.
27. What are the main features of a Payment Gateway Software?
28. What are the differences between Mobile Financial System (MFS) and Core Banking System (CBS)?
29. What services are available in Agent Banking System?
30. Which additional features other than the features in a core banking software should be available in Agent Banking Software?
31. What are the differences between a Core Banking and Agent Banking System?
32. List special devices required for Agent Banking operation.
33. What kind of application level securities to be incorporated in Agent Banking System?
34. Name 5 (five) Agent Banking Software available in Bangladesh.
35. What menu a customer gets to operate Agent Banking?

মডিউল-সি

# অলটারনেটিভ ডেলিভারি চ্যানেল এবং ফান্ড ট্রান্সফার সিস্টেম

অল্টারনেটিভ ডেলিভারি চ্যানেল হলো প্রথাগত শাখা নেটওয়ার্ক ছাড়া অন্য সব চ্যানেল, যা ব্যবহার করে ব্যাংক ক্লায়েন্টদের কাছে বিভিন্ন ব্যাংকিং সেবা পৌঁছে দেওয়া হয়। এই চ্যানেলগুলোর মধ্যে রয়েছে এটিএম, সিআরএম, ডিপোজিট মেশিন, পিওএস টার্মিনাল, ইন্টারনেট ব্যাংকি, এসএমএস অ্যালার্ট ব্যাংকি, ই-কমার্স, কল সেন্টার, মোবাইল ফিনান্সিয়াল সার্ভিস (এমএফএস) এবং এজেন্ট ব্যাংকি।

তহবিল স্থানান্তর নির্দেশাবলি পাঠানোর জন্য, অনেক ডিভাইস/সিস্টেম ব্যবহার করা হয়। এগুলো হলো টেলেক্স, সুইফট, ব্যাচ (BACH), বিএসিপিএস (BACPS), বিইএফটিএন (BEFTN), এনপিএসবি (NPSB), আরটিজিএস (RTGS), চিপস (CHIPS), ফেডওয়ার, ব্যাংকওয়্যার, ইত্যাদি।

এই মডিউলে আমরা বিভিন্ন বিকল্প ডেলিভারি চ্যানেল এবং ফান্ড ট্রান্সফার সিস্টেম নিয়ে আলোচনা করব।

## ১. অটোমেটেড টেলার মেশিন (ATM) এবং ক্যাশ রিসাইক্লিং মেশিন (CRM)

এটিএম/সিআরএম ব্যাংক কার্ড দিয়ে নগদ টাকা তোলা (এটিএম/সিআরএম) এবং ক্যাশ ডিপোজিট (শুধু সিআরএম) করার জন্য ব্যবহার করা হয়। এছাড়াও এটিএম/সিআরএম একটি কার্ডধারীকে অ্যাকাউন্টের বর্তমান অবস্থা জানাতে পারে (একটি কাগজে প্রিন্টসহ), এবং একটি অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে অর্থ স্থানান্তর করতে সাহায্য করে। কার্ড পড়ার জন্য এটিএম/সিআরএম এর সঙ্গে কার্ড পড়ার একটি ডিভাইস এবং কার্ডধারীর সঙ্গে যোগাযোগ করার জন্য ডিসপ্লে ও কীবোর্ড সরবরাহ করা হয়। এটিএম/সিআরএম এর সঙ্গে একটি কম্পিউটার সংযুক্ত থাকে, যা ক্যাশ ডিসপেন্সারের ব্যবস্থাপনা এবং এর স্টেটাস নিয়ন্ত্রণ করে থাকে। শেষটি বরং গুরুত্বপূর্ণ, কারণ ক্যাশ ডিনপেন্সার হলো নগদ টাকার ভাণ্ডার। এটিএম/সিআরএম-এর ক্যাসেটে বিভিন্ন মূল্যমানের নোট রাখা হয়, যা বিশেষ নিরাপদে থাকে। ক্যাসেটের সংখ্যা একটি এটিএম/সিআরএম দ্বারা সরবরাহকৃত এবং একটি সিআরএম দ্বারা গ্রহণকৃত বিভিন্ন মূল্যের নোটের সংখ্যা নির্ধারণ করে। যোগাযোগ প্রক্রিয়ার জন্য এটিএম/সিআরএম-এ মডেম বা ল্যান কার্ড সংযুক্ত থাকে।

বাংলাদেশে এটিএম/সিআরএম ব্যবহার শুধুমাত্র শহরেই সীমাবদ্ধ। বাংলাদেশে এটিএম/সিআরএম-এর সংখ্যা দ্রুত বৃদ্ধি পাচ্ছে, ২০০৩ সালে সংখ্যাটি ১০০টি থেকে ২০১০-এ ১৯০০-টি এবং ২০২১-এ সংখ্যাটি বেড়ে ১১,০০০-টিতে দাঁড়িয়েছে। ১১,০০০ এটিএম/সিআরএম-এর মধ্যে ডাচ্-বাংলা ব্যাংক একাই ৫,০০০ এটিএম/সিআরএম ইনস্টল করেছে। পরবর্তী বড় এটিএম/সিআরএম অধিগ্রহণকারীরা হলো ব্র্যাক ব্যাংক, ইসলামী ব্যাংক এবং কিউ-ক্যাশ নেটওয়ার্ক।

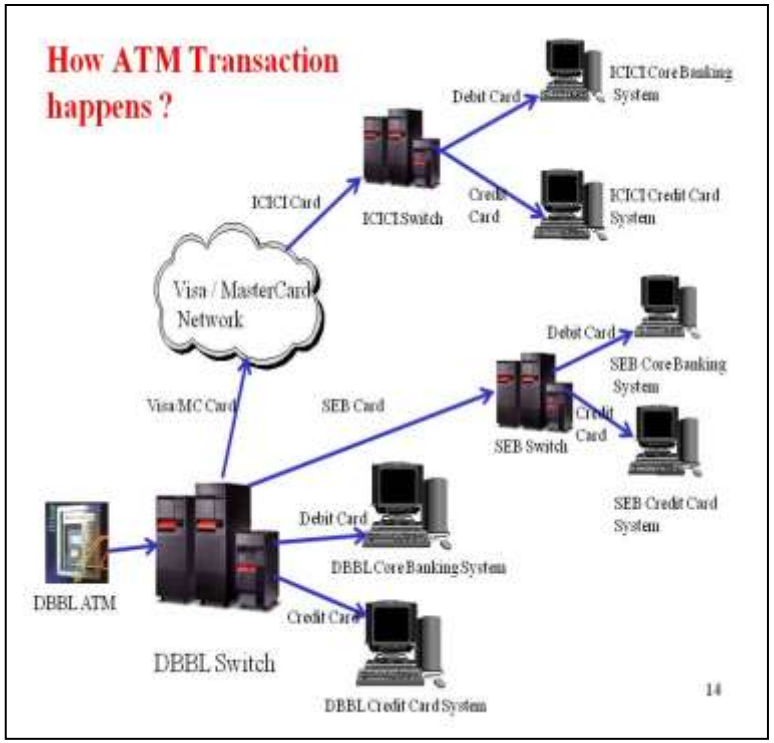
### ১.১. এটিএম/সিআরএম থেকে প্রাপ্ত পরিষেবা

কার্ডধারীরা এটিএম/সিআরএম ব্যবহার করে অনেক ব্যাংকি কার্যক্রম সম্পাদন করতে পারেন, যা নিচে তালিকাভুক্ত করা হয়েছে—

- নগদ উত্তোলন
- কার্ডবিহীন নগদ উত্তোলন
- নগদ জমা (শুধু সিঅরএম)
- এক অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে তহবিল স্থানান্তর
- আন্তঃব্যাংক তহবিল স্থানান্তর
- বৈদেশিক রেমিট্যান্স গ্রহণ
- ব্যালেন্স অনুসন্ধান
- অ্যাকাউন্টের স্টেটমেন্ট প্রিন্টিং
- চেক বই এর জন্য অনুরোধ পাঠানো
- ইউটিলিটি বিল পেমেন্ট
- মোবাইল রিচার্জ

*এটিএম*

**১.২. নগদ তোলার ক্ষেত্রে এটিএম/সিআরএম কীভাবে কাজ করে?**




সমস্ত এটিএম/সিআরএম ব্যাংকের ডেটা সেন্টারে একটি সুইচিং সফ্টওয়্যারের সঙ্গে সংযুক্ত থাকে। এটিএম/সিআরএম-এ কার্ড ঢোকানো হলে, কার্ড রিডার কার্ডের মেগ-স্ট্রাইপ বা চিপ থেকে কার্ড নম্বর, মেয়াদ শেষ হওয়ার তারিখ, ব্যাংকের আইডেন্টিফিকেশন নম্বর ইত্যাদি পড়ে, ব্যবহারকারীর কাছ থেকে পিন এবং টাকার পরিমাণ ইনপুট নেয় এবং সুইচিং সফ্টওয়্যার-এ এই তথ্যসমূহ প্রেরণ করে।

সুইচিং সফ্টওয়্যার তারপর কার্ডটি অন-আস বা অফ-আস কি না তা পরীক্ষা করে। যদি অন-আস হয় এবং কার্ডটি একটি ডেবিট কার্ড হয়, তাহলে সুইচিং সফ্টওয়্যারটি কার্ডের বৈধতা (কার্ডের নম্বর ডাটাবেসে বিদ্যমান আছে কি না, মেয়াদ শেষ হয়ে গেছে কি না, ইত্যাদি), স্ট্যাটাস (চুরি করা বা হট কার্ড কি না) এবং কার্ডের পিন পরীক্ষা করে। সমস্ত চেক পাস হলে, সংশ্লিষ্ট অ্যাকাউন্ট নম্বর এবং টাকার পরিমাণ অ্যাকাউন্ট থেকে ডেবিট করার অনুরোধসহ ব্যাংকের কোর ব্যাংকি সিস্টেমে প্রেরণ করে। যদি কোর ব্যাংকি সিস্টেম অ্যাকাউন্টে পর্যাপ্ত ব্যালেন্স খুঁজে পায় এবং অ্যাকাউন্টটি অপারেটিভ থাকে, তাহলে সমপরিমাণ টাকা অ্যাকাউন্ট থেকে ডেবিট করে এবং সুইচের মাধ্যমে এটিএম/সিআরএম-এ একটি অনুমোদন কোড পাঠায়। তারপর এটিএম/সিআরএম টাকা গণনা করে গ্রাহকদের কাছে প্রেজেন্ট করে।

যদি কার্ডটি অন-আস হয় এবং এটি একটি ক্রেডিট কার্ড হয়, তবে স্যুইচটি কোনো কিছু পরীক্ষা না করেই ক্রেডিট কার্ড সিস্টেমে তথ্য প্রেরণ করে। ক্রেডিট কার্ড সিস্টেম কার্ডের বৈধতা পরীক্ষা করে (কার্ড নম্বর ডাটাবেসে বিদ্যমান আছে কি না, মেয়াদ শেষ হয়ে গেছে কি না ইত্যাদি), স্ট্যাটাস (একটি চুরি বা হট কার্ড কি না) এবং কার্ডের পিন পরীক্ষা করে। যদি সমস্ত চেক পাস হয়ে যায় এবং কার্ড অ্যাকাউন্টে যথেষ্ট ক্রেডিট লিমিট থাকে, তাহলে ক্রেডিট কার্ড সিস্টেম সমপরিমাণ টাকা কার্ড অ্যাকাউন্ট থেকে ডেবিট করে এবং সুইচের মাধ্যমে এটিএম/সিআরএম-এ একটি অনুমোদন কোড পাঠায়। তারপর এটিএম/সিআরএম, টাকা গণনা করে তা গ্রাহকের কাছে প্রেজেন্ট করে।

যদি লেনদেন অফ-আস হয়, তাহলে সুইচ চেক করে যে লেনদেনটি বাংলাদেশের কোনো ব্যাংকের কার্ডহোল্ডার করেছেন কিনা। যদি কার্ডধারী বাংলাদেশের কোনো ব্যাংকের হয়, তাহলে বাংলাদেশ ব্যাংকের ( কেন্দ্রীয় ব্যাংক) ন্যাশনাল পেমেন্ট সিস্টেম, বাংলাদেশ (NPSB) এ প্রেরণ করে। এনপিএসবি কার্ডধারীর ব্যাংকের সুইচিং সফ্টওয়্যারে লেনদেন প্রেরন করে। ঐ ব্যাংকের সুইচিং সফ্টওয়্যার কার্ডের বৈধতা, স্থিতি, পিন ইত্যাদি যাচাই করে এবং কোর ব্যাংকি সিস্টেম (যদি ডেবিট কার্ড) বা ক্রেডিট কার্ড সিস্টেম (যদি ক্রেডিট কার্ড) থেকে অনুমোদন নিয়ে তা এনপিএসবি এর মাধ্যমে এটিএম/সিআরএম-এ প্রেরণ করে।

যদি লেনদেনটি অফ-আস হয় এবং কার্ডটি একটি আন্তর্জাতিক কার্ড হয়, তবে ব্যাংকের সুইচ এই লেনদেনটি যথাযথ পেমেন্ট অ্যাসোসিয়েশনের কাছে (ভিসা, মাস্টারকার্ড, জেসিবি, ইউনিয়ন পে ইত্যাদি) ফরোয়ার্ড করে। পেমেন্ট অ্যাসোসিয়েশন তার সদস্য ব্যাংকে লেনদেনটি ফরোয়ার্ড করে, যা কার্ডের বৈধতা, স্থিতি, পিন ইত্যাদি যাচাই করে এবং এর কোর ব্যাংকি সিস্টেম (যদি ডেবিট কার্ড) বা ক্রেডিট কার্ড সিস্টেম (যদি ক্রেডিট কার্ড) থেকে অনুমোদন নিয়ে তা পেমেন্ট অ্যাসোসিয়েশনের মাধ্যমে এটিএম/সিআরএম-এ প্রেরণ করে।

অনুমোদনের কোডটি পজিটিভ হলে, এটিএম/সিআরএম টাকা গণনা করে এবং গ্রাহককে উপস্থাপন করে।

## ১.৩. এটিএম/সিআরএম এর স্পেসিফিকেশন এবং এ সম্পর্কিত বিষয়াবলি

### ১.৩.১ এটিএম/সিআরএম স্পেসিফিকেশন

এটিএমের ধরন : বাংলাদেশে দুই ধরনের এটিএম পাওয়া যায়—লবি টাইপ এবং থ্রো-দ্য-ওয়াল টাইপ। লবি টাইপের এটিএম ইনস্টল করার জন্য ছোট জায়গা প্রয়োজন, যেখানে থ্রো-দ্য-ওয়াল টাইপের এটিএম-এর জন্য একটি ঘরে দুটি রুম সহ বড় জায়গার প্রয়োজন হয়। সামনের অংশ গ্রাহকদের জন্য ব্যবহার করা হয় এবং একটি পৃথক দরজা এবং এয়ার কন্ডিশনারের (এসি) ব্যবস্থা থাকে। পেছনের রুমে মেশিন বসানো হয় এবং এই রুমের জন্য একটি আলাদা দরজা এবং এসি থাকে। ক্যাশ পেছন দিক থেকে লোড করা হয়। একটি লবি টাইপের এটিএমের ক্ষেত্রে, এটিএমের সামনের দিক থেকে ক্যাশ লোড করা হয়।

এটিএম/সিআরএম উৎপাদনকারী : এটিএম/সিআরএম-এর শীর্ষ চারটি ব্র্যান্ড হলো : ডিবোল্ট, এনসিআর, হিটাচি, উইনকোর-নিক্সডর্ফ।


*এনসিআর এটিএম*


*ডাইবোল্ড এটিএম*

*উইঙ্কর নিক্সডর্ফ এটিএম*

কম্পিউটার : প্রতিটি এটিএম-এ একটি কম্পিউটার থাকে। কম্পিউটারের জন্য একটি আধুনিক প্রসেসর ব্যবহার করা হয়। এক জিবি র‍্যাম, ৮০ জিবি এইচডিডি, ১০/১০০ বেসটি ইথারনেট ইউএসবি, ইথারনেট অ্যাডাপ্টার ইত্যাদি কম্পিউটারের সঙ্গে সংযুক্ত থাকে। কম্পিউটারটি এটিএম চালু করে, ইলেকট্রনিকভাবে জার্নালের রেকর্ড সংরক্ষণ করে এবং 3 DES এনক্রিপশন সহ টিসিপি/আইপি প্রটোকল ব্যবহার করে লিজড্ লাইন, জিএসএম এবং ভি-স্যাট নেটওয়ার্কের মাধ্যমে ব্যাংকের সুইচিং সফটওয়্যারের যোগাযোগ করে।

ডিস্প্লে : ১৫" / ১৭" রঙিন ডিস্প্লে-এলসিডি বা টাচ স্ক্রিন।

**কার্ড রিডার :** কার্ড রিডার একটি এটিএম/সিআরএম-এর অত্যন্ত গুরুত্বপূর্ণ অংশ। এটি গ্রাহকদের কার্ডের মেগ-স্ট্রাইপ বা চিপ থেকে (ইএমভি কার্ড হলে) কার্ডের তথ্যাদি পড়ে থাকে।

**প্রোটোকল :** দুটি প্রোটোকল যথা এনডিসি+ এবং ডি৯১২ এর মাধ্যমে এটিএম সুইচের সঙ্গে যোগাযোগ করে থাকে।

**কী প্যাড :** এনক্রিপ্টেড/ইপিপি (পিসিআই কমপ্লায়েন্ট) কী সহ একটি স্ট্যান্ডার্ড কীবোর্ড এটিএম/সিআরএম-এর সঙ্গে ব্যবহার করা হয়।

**প্রিন্টার :** দুটি প্রিন্টার যথা কনজিউমার প্রিন্টার এবং জার্নাল প্রিন্টার একটি ATM/CRM এর সঙ্গে সরবরাহ করা হয়। কনজিউমার প্রিন্টার গ্রাহকদের জন্য প্রতিটি লেনদেন একটি স্লিপে প্রিন্ট করে এবং জার্নাল প্রিন্টার এটিএম/সিআরএম-এর ভিতরে থাকে এবং ব্যর্থ/সফল অবস্থাসহ সমস্ত লেনদেন প্রিন্ট করে। ক্যাশ ডেলিভারি সংক্রান্ত বিরোধ এই জার্নাল থেকে চিহ্নিত করা হয়। বর্তমান যুগে, এই কাগজের জার্নাল একটি ইলেকট্রনিক জার্নাল দ্বারা প্রতিস্থাপিত হয়েছে।

**ডিসপেনসার :** ডিসপেনসার এমন একটি ইউনিট, যা টাকা গণনা করে এবং বিতরণ করে। ডিসপেনসার ভ্যাকুয়াম পিক বা ফ্রিকশন পিক প্রযুক্তি ব্যবহার করে টাকা গণনা এবং বিতরণ করে থাকে।

**নিরাপত্তা :** এটিএম/সিআরএম ভল্টে ডুয়াল কম্বিনেশন লক দেওয়া আছে, ফলে ভল্ট খুলতে দুজন অফিসারের প্রয়োজন হয়। নিরাপদটি ২টি স্ট্যান্ডার্ডে পাওয়া যায় ইউএল ২৯১ এবং সিইএন। সিইএন ইউএল ২৯১ এর চেয়ে শক্তিশালী।

**সিআরএম-এ ক্যাশ গ্রহণ :** সিআরএম-এ ক্যাশ গ্রহণের সুবিধা রয়েছে। ক্যাশ বান্ডিল হিসাবে জমা করা হয়। সিআরএম বিভিন্ন মূল্যমানের নোট আলাদা আলাদাভাবে গণনা করে এবং ক্যাশ ডিসপেন্সিং ক্যাসেটে জমা করে। ফলে সিআরএম-এ ক্যাশ ভরার প্রয়োজন এটিএম-এর তুলনায় অনেক কম।

### ১.৩.২. এটিএম/সিআরএম-এ ব্যবহৃত নোটের মূল্যমান

এটিএম/সিআরএম-এ প্রাপ্ত বিভিন্ন মূল্যমানের নোটের সংখ্যা নির্ভর করে এটিএম/সিআরএম-এ কতগুলো ক্যাসেট ঢোকানো যেতে পারে তার ওপর। যদি একটি এটিএম/সিআরএম-এ ৪টি ক্যাসেট রাখার ব্যবস্থা থাকে, তাহলে ৪ ধরনের

কারেন্সি নোট এতে লোড করা যেতে পারে। যাইহোক, ঘন ঘন ক্যাশ লোডিং এড়াতে, ব্যাংকগুলো সাধারণত এটিএম/সিআরএম-এ শুধু এক বা দুটি মূল্যমানের নোট প্রদান করে, যেমন ২টি ক্যাসেটে ১০০০ টাকার নোট এবং অন্য ২টি ক্যাসেটে ৫০০ টাকার নোট। একটি ক্যাসেটে ২০০০টি নোট রাখা যায়। এই ভাবে যদি দুটি ক্যাসেট ১০০০ টাকার নোট এবং অন্য দুটিতে ৫০০ টাকার নোট লোড করা হয়, তাহলে একটি এটিএম/সিআরএম-এ একবারে ৬.০০ মিলিয়ন টাকা লোড করা যেতে পারে।

### ১.৩.৩. তৃতীয় পক্ষ দ্বারা ক্যাশ ফিডিং

১০০০টি এটিএম এবং ১ মিলিয়ন কার্ডের আকারসহ একটি ব্যাংকের এটিএমে প্রতিদিন ৫০০ মিলিয়ন টাকা লোড করতে হবে। কিন্তু সিআরএম-এ ক্যাশ ভরার পরিমাণ অনেক কম। কখনও কখনও নগদ জমার পরিমাণ নগদ উত্তোলনের চেয়ে বেশি হলে সিআরএম থেকে ক্যাশ সরানোর প্রয়োজন হতে পারে।

আমাদের দেশে নোটের মান ভালো না হওয়ায় এবং নোটে ছিদ্র থাকায়, এটিএম-এ ক্যাশ ফিড করার আগে একে একে সব নোট চেক করতে হয়, খারাপ নোট ম্যানুয়ালি প্রত্যাখ্যান করতে হয় এবং তারপর নোটগুলোকে এমনভাবে সাজিয়ে রাখতে হয় যেন দুটি সংলগ্ন নোটের গর্ত দুটি বিপরীত দিকে পড়ে। এর জন্য প্রতিদিন বিপুল জনবলের প্রয়োজন হয়। এজন্য এই কাজটি তৃতীয় পক্ষের কাছে আউটসোর্স করা হয়। তবে, এটিএম-এর পরিবর্তে সিআরএম ইনস্টল করা হলে এই কার্যক্রম উল্লেখযোগ্যভাবে হ্রাস পেয়েছে।

### ১.৩.৪. ক্যাশের পার্সিয়াল ডিসপেনচ (Partial Dispence) ও নন-ডিসপেনচ (Non-Partial Dispence)

কখনও কখনও এটিএম/সিআরএম-এর ভেতরে লোড করা নোটের গুণমানের কারণে, এটিএম/সিআরএম গ্রাহকের চাওয়া সমস্ত নোট গণনা করতে পারে না। এই ধরনের ক্ষেত্রে এটিএম/সিআরএম হয় অর্থের একটি অংশ বিতরণ করে বা কিছুই দেয় না। ফলে এটিএম/সিআরএম সুইচের মাধ্যমে অনুমোদনকারীর ব্যাংক বা সিস্টেমের কাছে একটি রিভার্সাল অনুরোধ পাঠায় এবং ব্যাংক এর সিস্টেম অ-বিতরণকৃত টাকার পরিমাণ গ্রাহকের অ্যাকাউন্টে ক্রেডিট করে দেয়।

কখনও কখনও, রিভার্সাল অনুরোধও ব্যর্থ হয় এবং গ্রাহক তার অ্যাকাউন্টে অর্থ ফেরত পান না। কার্ডধারীকে এক্ষেত্রে, কার্ড ইস্যুকারী ব্যাংকে রিপোর্ট করতে হবে। যেহেতু কার্ডধারী অ্যাকোয়ারিং ব্যাংকের সঙ্গে পরিচিত নয় এবং অ্যাকোয়ারিং ব্যাংকের গ্রাহক অ্যাকাউন্টে অ্যাক্সেস নেই, তাই তারা এই বিষয়ে কোনো পদক্ষেপ নিতে পারে না।

### ১.৩.৫. টাকা ক্যাপচার (Capture of Money)

কাস্টমারের কাছে টাকা প্রেজেন্ট করার পর এটিএম/সিআরএম ৪৫ সেকেন্ডের জন্য অপেক্ষা করে (কাস্টমাইজেবল)। এই সময়সীমার মধ্যে গ্রাহক টাকা গ্রহণ না করলে এটিএম/সিআরএম টাকা ক্যাপচার করে এবং 'রিজেক্ট বিন' নামে একটি ক্যাসেটে সংরক্ষণ করে।

### ১.৩.৬. সংযোগের জন্য ব্যবহৃত নেটওয়ার্ক

একটি লেনদেন পরিচালনা করার জন্য এটিএম/সিআরএম-এর শুধু ১৬ কেবিপিএস ব্যান্ডউইথ প্রয়োজন। ফলে এটিএম/সিআরএম লেনদেনের জন্য যেকোনো ধরনের যোগাযোগ মাধ্যম ব্যবহার করা যেতে পারে। এটিএম/সিআরএম লেনদেনের জন্য সবচেয়ে সহজ এবং সস্তা মাধ্যম হলো মোবাইল ডেটা নেটওয়ার্ক। কিন্তু, ব্যাংকগুলো সাধারণত ডেটা সংযোগের জন্য ফাইবার অপটিক ব্যবহার করে কারণ এটি যোগাযোগের জন্য সবচেয়ে নির্ভরযোগ্য মাধ্যম।

### ১.৩.৭. কার্ড ক্যাপচার এবং হট কার্ড (Card Capture and Hot-card)

নিরাপত্তার কারণে, যদি একজন কার্ডধারী ৩ বার ভুল পিন ঢোকান, এটিএম/সিআরএম কার্ডটি ক্যাপচার করে এবং কার্ডটি 'হট' হয়ে যায়। এই ধরনের ক্ষেত্রে, গ্রাহককে তার হোম ব্রাঞ্চে রিপোর্ট করতে হয়। ক্যাশ লোডিং দল, তাদের পরবর্তী সফরের সময়, কার্ডটি সংগ্রহ করে এবং অ্যাকুয়ারিং ব্যাংকে পাঠায়। এটিএম/সিআরএম-এ যদি একটি হট কার্ড ঢোকানো হয়, এটিএম/সিআরএম তৎক্ষনাৎ কার্ডটি ক্যাপচার করবে। অতএব, হট কার্ড ব্যবহার করার আগে ব্যাংকের হেল্প ডেস্কে কল করা এবং কার্ডের স্টেটাস স্বাভাবিক করা প্রয়োজন। আপনার কলের সময়, আপনি যে কার্ডধারী তা নিশ্চিত করার জন্য ব্যাংক অফিসার আপনাকে বেশ কিছু প্রশ্ন করতে পারেন। কার্ড ক্যাপচার করার অন্যান্য কারণ হলো এটিএম/সিআরএম-এ পাওয়ার ফেইলিউর (বা ইউপিএস ব্যাকআপ শেষ হওয়ার কারণে), কার্ডটি পূর্বেই ব্লক হয়ে গিয়েছিল এবং এটিএম/সিআরএম-এর কার্ড রিডারের সমস্যা।

### ১.৩.৮. এটিএম/সিআরএম বুথের জন্য এককালীন এবং মাসিক খরচ

এটিএম/সিআরএম বুথে এককালীন বিনিয়োগ নিম্নরূপ—

- এটিএম/সিআরএম-এর দাম।
- জায়গার বাড়িওয়ালার কাছে অগ্রিম।
- ইউপিএস, সিসিটিভি, এয়ার কন্ডিশনার এর দাম।

- বুথ, সাইনেজ ও সাজসজ্জা নির্মাণের খরচ।

মাসিক খরচ নিম্নরূপ—

- বুথের ভাড়া
- বিদ্যুৎ খরচ
- ৩ শিফটে নিয়োজিত ৩ জন সিকিউরিটি গার্ডের বেতন
- ক্যাশ সর্টিং এবং ফিডিং চার্জ
- লিঙ্ক চার্জ
- এটিএম/সিআরএম, ইউপিএস, সিসিটিভি, এসি এবং বুথের জন্য রক্ষণাবেক্ষণ চার্জ
- আনুপাতিক হারে সুইচিং সিস্টেমের খরচ
- আনুপাতিক হারে ডেটা সেন্টারের জনবল এবং রক্ষণাবেক্ষণ খরচ

প্রতি এটিএম/সিআরএম-এ এককালীন খরচ ২.০০-২.৫০ মিলিয়ন টাকার মধ্যে হতে পারে এবং মাসিক খরচ এটিএম/সিআরএম প্রতি ৮০,০০০-১০০,০০০ টাকার মধ্যে হতে পারে।

### ১.৩.১০. এটিএম/সিআরএম থেকে আয়

সাধারণত এটিএম/সিআরএম-এ অন-আস লেনদেনের জন্য কোনো লেনদেন ফি নেই। তবে অফ-আস লেনদেনের জন্য, অ্যাকুয়ারিং ব্যাংক প্রতিটি স্থানীয় লেনদেনের জন্য ২০ টাকা এবং প্রতিটি আন্তর্জাতিক লেনদেনের জন্য ইউএসডি ১.০০-১.২৫ পাবে। এগুলোকে যথাক্রমে স্থানীয় এবং আন্তর্জাতিক এটিএম/সিআরএম ইন্টারচেঞ্জ ফি বলা হয় এবং বাংলাদেশ ব্যাংক এবং সংশ্লিষ্ট পেমেন্ট অ্যাসোসিয়েশন দ্বারা নির্ধারিত হয়। কার্ডহোল্ডারদের কাছ থেকে আদায়কৃত ডেবিট কার্ডের বার্ষিক ফি ব্যাংকের প্রধান আয় হিসেবে ধরা যেতে পারে।

## ১.৪. এটিএম/সিআরএম জালিয়াতি এবং প্রতিকার (ATM/CRM Fraud and remedy)

বিগত কয়েক বছরে সারা বিশ্বে এটিএম/সিআরএম জালিয়াতি উল্লেখযোগ্যভাবে বৃদ্ধি পেয়েছে এবং কার্ড ও পিন-এর তথ্য চুরি করার প্রযুক্তি আবিষ্কৃত হওয়ায় তা আরও বিকশিত হয়েছে। এটিএম/সিআরএম জালিয়াতি সাধারণত দুটি প্রকারে সংঘটিত হয়। কার্ড রিডিং ডিভাইস এবং কার্ড-ট্র্যাপিং ডিভাইসের মাধ্যমে।

### ১.৪.১. কার্ড রিডিং ডিভাইস (Card-Reading Device)

অপরাধীরা প্রথমে এটিএম/সিআরএম-এ একটি স্কিমিং মেশিন এবং একটি মিনি-ক্যামেরা যোগ করে। কার্ড এন্ট্রি স্লটে মাউন্ট করা স্কিমিং ডিভাইস কার্ডের বার কোড পড়ে আর কার্ডধারী যখন তার পিন প্রবেশ করেন তখন মিনি ক্যামেরা পিন রেকর্ড করে। কার্ডধারী তার লেনদেন সম্পূর্ণ করার পরে কার্ডটি নিয়ে চলে যান। কিন্তু হ্যাকার তার কার্ডের তথ্য এবং তার পিন পেয়ে যায়। সাধারণত, প্রতারক একটি নতুন কার্ড তৈরি করে এবং গ্রাহকের অ্যাকাউন্ট থেকে অর্থ উত্তোলনের জন্য এটি ব্যবহার করে। স্কিমিং ডিভাইসগুলো সবসময় সহজে ধরা পড়ে না, বিশেষ করে যদি গ্রাহকরা এটিএম/সিআরএম-এর চেহারার সঙ্গে অপরিচিত হন।

আজকাল সমস্ত এটিএম/সিআরএম অ্যান্টি-স্কিমিং ডিভাইসসহ তৈরি করা হয়, যা কার্ড ঢোকানোর সময় কম্পন সৃষ্টি করে। এই কম্পন একটি স্কিমিং মেশিন ইনস্টল করে স্কিমারের দ্বারা কার্ডের তথ্য পড়া এবং রেকর্ডিং প্রতিরোধ করে। যদি পুরোনো এটিএম/সিআরএম-এ অ্যান্টি-স্কিমিং ডিভাইস ইনস্টল না থাকে, তাহলে ব্যাংকগুলোকে আলাদা অ্যান্টি-স্কিমিং ডিভাইস কেনা উচিত এবং সেগুলো এটিএম/সিআরএম-এর সঙ্গে সংযুক্ত করা উচিত।

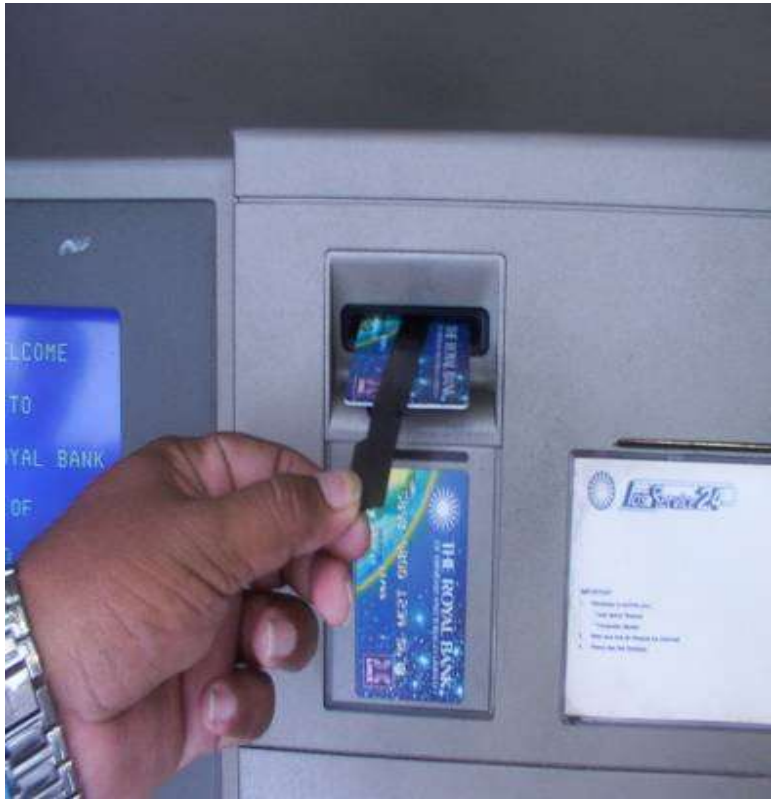
*সাধারণ এটিএম ডিভাইস*

*কার্ড স্লটের সামনে একটি স্কিমিং ডিভাইস যুক্ত এটিএম। লক্ষ্য করুন কীভাবে কার্ড স্লটটি বাইরের দিকে ফুলে আছে।*

### ১.৪.২ কার্ড ট্র্যাপিং ডিভাইস (Card-Trapping Device)

এটিএম/সিআরএম পরিবর্তন করার একটি বিকল্প রূপ হলো কার্ড স্লটে এক্স-রে টেপের একটি পাতলা ফিতা ঢোকানো। ফিতাটি গ্রাহকের কার্ডকে আটকে রাখে

এবং মনে হয় যেন কার্ডটি কাজ করছে না। এই মুহূর্তে, অন্য কেউ, একজন প্রতারক আসে এবং কার্ডধারককে বলে যে সে (কার্ডধারী) তার (কার্ডধারীর) পিন কোড পুনরায় প্রবেশ করে তার কার্ড পুনরুদ্ধার করতে পারে। কার্ডধারী যখন তার পিন টাইপ করে, তখন প্রতারক তা দেখে ফেলে। কার্ডটি এখনও বের না হওয়ায় কার্ডধারী এটিএম/সিআরএম থেকে চলে যায়। তারপর প্রতারক কার্ডটিসহ ডিভাইসটি বের করে নেয়। পরে কার্ডধারীর ঐ কার্ড ও পিন ব্যবহার করে এটিএম/সিআরএম থেকে টাকা উঠায়ে নেয়।



*কার্ড-ট্র্যাপিং ডিভাইস (device)*

এই ধরনের স্ক্যামের শিকার হওয়া প্রতিরোধ করার জন্য—

- গ্রাহকদিগকে সেই সব এটিএম/সিআরএম ব্যবহার করা থেকে বিরত থাকতে হবে যেখানে কার্ড রিডিং ডিভাইস বা কার্ড ট্র্যাপিং ডিভাইস মাউন্ট করা হয়েছে বলে মনে হবে। কার্ড এন্ট্রি স্লটগুলো এটিএম/সিআরএমের পৃষ্ঠের সঙ্গে ফ্লাশ করা অবস্থায় থাকা উচিত। যদি একজন গ্রাহক একটি কার্ড এন্ট্রি স্লট দেখেন, যা মেশিনের ওপরে উত্থিত হয়েছে, তাহলে এটি সন্দেহের জন্ম দেবে এবং ব্যবহার করা উচিত নয়।
- গ্রাহক যদি স্ক্রিন পড়তে বা পিন লিখতে অস্বস্তিকর মনে করেন, তাহলে তার মেশিনটি ব্যবহার করা উচিত নয়। হয়ত এটা পরিবর্তন করা হয়েছে। এটিএম/সিআরএম-এর স্ক্রিনের পাশে কোন ডিসপ্লে কখনও মাউন্ট করা হয় না। যেকোনো কিছু যা একটি এটিএম/সিআরএম এর কিছুকে ব্লক করে বা আংশিকভাবে অস্পষ্ট করে, তাতে একটি ক্যামেরা লুকানো থাকতে পারে।
- গ্রাহককে তার পিনটি সতর্কতার সঙ্গে ব্যবহার করতে হবে, বিশেষ করে এটি প্রবেশ করার সময়, তার একটি হাত দিয়ে কীপ্যাডটি ঢেকে রাখতে হবে।
- যদি একটি মেশিন কার্ডটি গ্রাস করে, গ্রাহককে তৎক্ষণাৎ ব্যাংকের হেল্প ডেস্কে কল করে রিপোর্ট করতে হবে।
- গ্রাহককে তার নতুন কার্ড পাওয়ার সময় সঙ্গে দেওয়া পিন নম্বর পরিবর্তন করতে হবে। গ্রাহকের কার্ড এবং পিন একসঙ্গে রাখা উচিত নয়।
- ব্যাংকগুলোকে বিল্ট-ইন অ্যান্টি-স্কিমিং ডিভাইসসহ এটিএম/সিআরএম কেনা এবং ইনস্টল করা উচিত। পুরোনো যে সমস্ত এটিএম/সিআরএমে কোনো অ্যান্টি-স্কিমিং ডিভাইস ইন্টিগ্রেটেড নেই, ব্যাংক আলাদা অ্যান্টি-স্কিমিং ডিভাইস কিনে এই সমস্ত এটিএম/সিআরএম-এ ইনস্টল করতে পারে।

## ২. ডিপোজিট মেশিন

একটি ডিপোজিট মেশিন হলো ব্যাংক কর্তৃক ইনস্টল করা একটি মেশিন যাহা অর্থ জমা দেওয়ার জন্য গ্রাহকগণ ব্যবহার করেন। ডিপোজিট মেশিনকে KIOSK ও বলা হয়। একটি ডিপোজিট মেশিনে একটি কার্ড রিডার থাকে। যদি কোনো কার্ডধারী টাকা জমা দেওয়ার আগে তার কার্ড ঐ কার্ড রিডারে প্রবেশ করায় তাহলে তাকে তার অ্যাকাউন্ট নম্বর বা কার্ড নম্বর টাইপ করতে হবে না। জমা করার জন্য আনা টাকা একটি বন্ধ খামে ঢোকানো হয় এবং মেশিনের ভেতরে ফেলে দেওয়া হয়। ডিপোজিট মেশিনের কীবোর্ড ব্যবহার করে জমা করা টাকার পরিমাণ এন্ট্রি দেওয়া হয়।

কখনও কখনও, খামের ভিতরে ঢোকানো টাকা ও এন্ট্রি দেওয়ার পরিমাণ ভিন্ন হতে পারে। সিসিটিভির কভারেজের মধ্যে ব্যাংকের একটি দল খামগুলো খুলে। বিরোধ দেখা দিলে দলের (ব্যাংক কর্মকর্তাদের) সিদ্ধান্তই চূড়ান্ত বলে গণ্য হবে। তবে গ্রাহক অসম্মত হলে গ্রাহক সিসিটিভি রেকর্ড দেখতে পারেন।

যাইহোক, কিছু ব্যাংক, এই ধরনের বিরোধ এড়াতে, খামের ভিতরে পরিমাণ নিশ্চিত করার জন্য প্রতিটি ডিপোজিট মেশিনের বুথে ব্যাংক কর্মকর্তাদের নিযুক্ত করে। ডিপোজিট মেশিনে ফেলার আগে টাকার পরিমাণ ও খামে উল্লিখিত টাকার পরিমাণ মিলিয়ে ব্যাংকের কর্মকর্তা ও গ্রাহক উভয়েই খামের ওপর স্বাক্ষর করে থাকেন।

একটি ডিপোজিট মেশিনের গুরুত্বপূর্ণ অংশ হলো একটি ভল্ট, এর স্পেসিফিকেশন (ইউএল বা সিইএন) এবং এর নোট ধারণক্ষমতা। ভল্টের ধারণক্ষমতা এত বড় হতে পারে যে প্রতিটি খামে ৫০০টি নোট সংবলিত ৭০০টি খাম ধারণ করতে পারে।

ডিপোজিট মেশিনটি একটি কম্পিউটার, মনিটর এবং সফ্টওয়্যার দিয়ে সজ্জিত। বাংলাদেশে স্থানীয়ভাবে ডিপোজিট মেশিন তৈরি করা হয়।

### ৩. ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথ

ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথ হলো একটি অনন্য ধারণা যা ডাচ-বাংলা ব্যাংক তার গ্রাহকদের জন্য তৈরি করেছে। নিম্নলিখিতগুলো একটি ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে ইনস্টল করা থাকে—

- বেশ কয়েকটি (২-৫) এটিএম
- বেশ কয়েকটি সিআরএম/ডিপোজিট মেশিন (১-৩)
- দুই শিফটে একজন করে কর্মকর্তা
- কয়েকটি ইউপিএস
- বিভিন্ন নেটওয়ার্ক প্রদানকারী কর্তৃক স্থাপিত ডেটা লিঙ্ক।

এটিএম/সিআরএমগুলো সাধারণত নিম্নলিখিত কারণে অকেজো হয়ে যেতে পারে—

- ব্যাংক সার্ভারের সঙ্গে সংযুক্ত লিঙ্ক সচল নয়।
- এটিএম/সিআরএম-এর ভিতরে টাকা নেই।
- নোংরা নোটের কারণে টাকা জ্যাম হয়ে যায় যা পরবর্তী গ্রাহকদের টাকা তুলতে বাধা দেয়।
- এটিএম/সিআরএম হার্ডওয়্যার সমস্যা।
- ইউপিএস সচল নয়।
- বিদ্যুৎ নেই।

উপরোক্ত সমস্যাসমূহ দূর করতে ডাচ-বাংলা ব্যাংক ফাস্ট ট্র্যাক স্থাপন করেছে। ব্র্যাক ব্যাংক এবং স্ট্যান্ডার্ড চার্টার্ড ব্যাংকও একই ধারণা নিয়ে ইলেকট্রনিক বুথ স্থাপন করেছে।

একটি ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথের কার্যক্রম নিচে উল্লেখ করা হলো—

#### ক. নগদ উত্তোলন

গ্রাহকরা ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে স্থাপিত ২ থেকে ৫টি এটিএম/সিআরএম-এর যে কোনো একটি থেকে টাকা তুলতে পারবেন। এটিএম/সিআরএমগুলো বিভিন্ন ইউপিএস থেকে চালিত হয় এবং বিভিন্ন লিঙ্ক প্রদানকারীর মাধ্যমে ডেটা সেন্টারের সঙ্গে সংযুক্ত থাকে, যা বৈদ্যুতিক এবং নেটওয়ার্ক সমস্যার জন্য রিডানডেন্সি তৈরি করে। আবার ফাস্ট ট্র্যাকে একাধিক এটিএম/সিআরএম-এর কারণে, এটিএম/সিআরএম এর অচল অবস্থা, টাকার ঘাটতি এবং টাকা জ্যামের ক্ষেত্রে প্রয়োজনীয় রিডানডেন্সি নিশ্চিত করা হয়েছে। এটি নিশ্চিত করে যে, একজন গ্রাহক অবশ্যই ফাস্ট ট্র্যাকে এটিএম/সিআরএম থেকে টাকা তুলতে সক্ষম হবেন। অন্যদিকে, ফাস্ট ট্র্যাকে একজন অফিসারের উপস্থিতি গ্রাহককে টাকা বা কার্ড ক্যাপচারের মতো যেকোন সমস্যার তৎক্ষণাৎ সমাধান করতে সাহায্য করে।

#### খ. টাকা জমা করা

একজন গ্রাহক ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে টাকা জমা দিতে পারেন এবং টাকা জমা দেওয়ার জন্য ব্যাংকের কাউন্টারে দীর্ঘ লাইন এড়াতে পারেন। গ্রাহক অর্থ জমা করার জন্য ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে অনেক রাত্রি অবধি সেবা পেতে পারেন। গ্রাহকরা সরাসরি CRM-এ টাকা জমা দিতে পারেন বা একটি ডিপোজিট খাম ব্যবহার করে ক্যাশ ডিপোজিট মেশিনেও টাকা জমা দিতে পারেন। ক্যাশ ডিপোজিট মেশিনের ক্ষেত্রে, ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে দায়িত্বরত কর্মকর্তা গ্রাহকদের কাছ থেকে নগদ টাকা বা চেক গ্রহণ করেন, টাকা গণনা করেন, এটি একটি খামে ঢোকান, খামটি বন্ধ করেন এবং খামে স্বাক্ষর করেন। গ্রাহকও খামে স্বাক্ষর করেন এবং খামটি ডিপোজিট মেশিনে ফেলে দেন। টাকা জমা দেওয়ার জন্য যদি CRM ব্যবহার করা হয়, তাহলে গ্রাহকের অ্যাকাউন্টে তাৎক্ষণিকভাবে টাকা জমা হয় এবং যদি ডিপোজিট মেশিন ব্যবহার করা হয়, তাহলে গ্রাহকের অ্যাকাউন্টে পরের কার্যদিবসে টাকা জমা হয়।

#### গ. অ্যাকাউন্ট খোলা

ডিউটি অফিসার গ্রাহকদের অ্যাকাউন্ট খোলার জন্য গ্রাহকের eKYC ফরম পূরণ করতে সহায়তা করে থাকেন। অফিসার সঙ্গে সঙ্গে গ্রাহকের অ্যাকাউন্ট নম্বর এবং

ডেবিট কার্ড হস্তান্তর করে থাকেন। এছাড়াও গ্রাহক CRM ব্যবহার করে তার অ্যাকাউন্টে তাৎক্ষণিক টাকা জমা করতে পারেন।

**ঘ. গ্রাহকের রিকোয়েস্ট ফর্ম**

গ্রাহকের বিভিন্ন প্রকার 'রিকোয়েস্ট ফর্ম' ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে পাওয়া যায়। কর্মরত কর্মকর্তা গ্রাহককে উপযুক্ত ফর্ম প্রদান, ফর্ম পূরণে সহায়তা করা, গ্রাহকের কাছ থেকে ফর্ম গ্রহণ এবং গ্রাহকের অনুরোধ বাস্তবায়নের জন্য প্রধান অফিস বা শাখার সংশ্লিষ্ট বিভাগে তা প্রেরণ করে। এই ধরনের সেবাগুলোর একটি তালিকা নিচে দেওয়া হলো—

i গ্রাহকরা একটি 'অ্যাকাউন্ট ট্রান্সফার' ফর্ম পূরণ করতে পারেন এবং অন্য অ্যাকাউন্টে ফান্ড ট্রান্সফারের জন্য ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথ অফিসারের কাছে হস্তান্তর করতে পারেন।

ii গ্রাহকরা একটি 'নতুন কার্ড' পাওয়ার জন্য একটি ফর্ম পূরণ করতে পারেন এবং একটি নতুন ডেবিট কার্ড (মাস্টারকার্ড ডেবিট/মায়েস্ট্রো/ভিসা ডেবিট/ভিসা ইলেক্ট্রন) বা ক্রেডিট কার্ড (মাস্টারকার্ড/ভিসা) পাওয়ার উদ্দেশ্যে তা তিনি ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে কর্মরত অফিসারের কাছে হস্তান্তর করতে পারেন।

iii গ্রাহকরা একটি 'কার্ড প্রতিস্থাপন' ফর্ম পূরণ করতে পারেন এবং এটিকে ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে কর্মরত অফিসারের কাছে হস্তান্তর করতে পারেন। একটি কার্ড (ডেবিট/ক্রেডিট) নিম্নলিখিত কারণে **সাধারণত** প্রতিস্থাপন করা হয়ে থাকে—

- কার্ড হারিয়ে/চুরি হয়ে গেলে।
- কার্ডে ভুল নাম/বানান ভুল থাকলে।
- কার্ডে ভুল ছবি সংযোজন করলে।
- কার্ডটি কোনো কারণে ভেঙে গেলে বা ক্ষতিগ্রস্ত হলে।
- কার্ড বা কার্ডের মেগনেটিক স্ট্রিপ ত্রুটিপূর্ণ হলে।
- ফাস্ট ট্র্যাক অফিসারের কাছে গ্রহণযোগ্য অন্য যে কোনো কারণে

iv গ্রাহকরা একটি 'ব্লক/আনব্লক কার্ড' নামক ফর্ম পূরণ করতে পারেন এবং এটিকে ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথ অফিসারের কাছে হস্তান্তর করতে পারেন তার কার্ডটি ব্লক করার জন্য বা ব্লক করা কার্ড পুনরায় সক্রিয় করার জন্য। নিম্নলিখিত যেকোনো কারণে একটি কার্ড ব্লক করা হতে পারে—

- এটিএম বা পিওএস টার্মিনালে পর পর তিন বার ভুল পিন প্রবেশ করানো হলে।
- গ্রাহক নিজেই কার্ড সেন্টারে ফোন করে অনুরোধের মাধ্যমে কার্ডটি ব্লক করেছেন।

v গ্রাহক পিন পুনরায় ইস্যু করার জন্য একটি অনুরোধ করতে পারেন। একজন গ্রাহক পিন পুনরায় ইস্যু করার জন্য তখনই অনুরোধ করতে পারেন, যখন যিনি তার পিনটি ভুলে গেছেন বা তার পিন অন্য কোনো ব্যক্তির দ্বারা আপস হয়েছে বলে তিনি মনে করেন।

vi গ্রাহক তার বিদ্যমান কার্ডের সঙ্গে একটি নতুন অ্যাকাউন্ট লিঙ্ক করার জন্য অনুরোধ করতে পারেন।

vii তাছাড়া গ্রাহক ক্রেডিট কার্ড অ্যাকাউন্টে নিম্নলিখিত সেবাগুলোর জন্য একটি অনুরোধ করতে পারেন—

- অটো ডেবিট স্থাপন করার জন্য।
- কার্ডের লিমিট বৃদ্ধি করার জন্য।
- সাপ্লিমিন্টারি কার্ড প্রাপ্তির জন্য।
- কার্ডটি বাতিল করার জন্য।
- কার্ড চেক পাওয়ার জন্য।

viii গ্রাহকের অ্যাকাউন্ট ডেবিট করা হয়েছে, কিন্তু গ্রাহক এটিএম/সিআরএম থেকে টাকা পান নাই। অনুরূপ না পাওয়া টাকা ফেরতের জন্য তিনি একটি অনুরোধ করতে পারেন।

ix গ্রাহক তার ব্যাংক অ্যাকাউন্টে ইন্টারনেট, এসএমএস এবং অ্যালার্ট সুবিধা পাওয়ার জন্য আবেদনপত্র জমা দিতে পারেন।

**ঙ ক্যাপচার কার্ড গ্রাহককে ফেরত প্রদান**

যদি ফাস্ট ট্র্যাক/ইলেক্ট্রনিক বুথে অবস্থিত কোন এটিএম/সিআরএম-এ গ্রাহকের কোনো কার্ড ক্যাপচার হয়ে যায়, ডিউটি অফিসার এটিএম-এর উপরের চেম্বারটি খুলে তা থেকে ক্যাপচার করা কার্ডটি সংগ্রহ করেন। তারপর তিনি কার্ডের পেছনে রেকর্ড করা ছবি এবং গ্রাহকের স্বাক্ষর চেক করার পর তাৎক্ষণিকভাবে কার্ডধারকের কাছে কার্ডটি ফেরত দেন।

## ৪. পিওএস টার্মিনাল (POS terminal)

### ৪.১. একটি পিওএস টার্মিনাল কী?

পিওএস মানে পয়েন্ট অব সেল। একটি POS টার্মিনাল হলো একটি ছোট ডিভাইস যা একটি ব্যাংক দ্বারা দোকান, হোটেল এবং ব্যবসায়ীর অফিসে ইনস্টল করা হয়।

গ্রাহক মার্চেন্টের কাছ থেকে পণ্য ও পরিষেবা কেনেন এবং যদি তার ডেবিট/ক্রেডিট কার্ড ব্যবহার করে বিল পরিশোধ করতে চান, তবে ব্যবসায়ী গ্রাহকের কার্ডটি POS ডিভাইসে সোয়াইপ বা ইনচার্ট করে বিলটি নিষ্পত্তি করেন। পিওএস টার্মিনালগুলো ম্যাগনেটিক স্ট্রিপ এবং চিপ সংবলিত ডেবিট/ক্রেডিট কার্ড ব্যবহার করে মার্চেন্ট অবস্থানে লেনদেন প্রক্রিয়াকরণের উদ্দেশ্যে তৈরি করা হয়ে থাকে। পিওএস টার্মিনালগুলোর কনফিগারেশন বিভিন্ন রকমের হতে পারে, তবে, সাধারণত একটি আধুনিক টার্মিনালে চিপ কার্ড এবং ম্যাগনেটিক স্ট্রিপ কার্ড পড়ার সুবিধা থাকে এবং পিন প্যাড, প্রিন্টার বা কম্পিউটার ও ক্যাশ রেজিস্টার সংযোগের জন্য কিছু পোর্ট থাকে।

এছাড়াও পিওএস টার্মিনালটির সঙ্গে একটি মডেম সংযুক্ত থাকে, যা ডেটা সেন্টারে কল ব্যাক করার ক্ষমতা রাখে। পিওএস টার্মিনালে প্রোগ্রাম তৈরি করা যেতে পারে। ফলে এটি কার্ডের অনলাইন অথরাইজেশন প্রদান করে থাকে। অবশেষে, ডেটা সেন্টারের সঙ্গে যোগাযোগ স্থাপিত হয়। সংযোগের একটি অধিবেশন চলাকালীন, পিওএস টার্মিনাল ডেটা সেন্টারের সার্ভার দ্বারা প্রেরিত তথ্য গ্রহণ করতে এবং মনে রাখতে পারে।


*পিওএস টার্মিনাল*

একটি পিওএস টার্মিনাল একটি পিএসটিএন লাইন বা জিপিআরএস ব্যবহার করে ডেটা সেন্টারের সঙ্গে যোগাযোগ করতে পারে। পিএসটিএন ধরনের পিওএস টার্মিনাল ডেটা সেন্টারের সঙ্গে যোগাযোগের জন্য একটি টেলিফোন লাইনের প্রয়োজন হয়, যেখানে জিপিআরএস ধরনের পিওএস টার্মিনাল ডেটা সেন্টারের সঙ্গে যোগাযোগের জন্য মোবাইল সিম কার্ড ব্যবহার করে থাকে। যখন একটি কার্ড সোয়াইপ করা হয় (যদি কার্ডটি মেগ-স্ট্রাইপ হয়) বা ইনচার্ট করা হয় (যদি কার্ডটি EMV হয়) পিওএস টার্মিনালটি একটি সেট করা নম্বরে ডায়াল করে এবং ডেটা সেন্টারের মডেম পুলের সঙ্গে সংযুক্ত হয় (যাকে NAC বা নেটওয়ার্ক অ্যাক্সেস কন্ট্রোলার বলা হয়)। সংযোগের পরে, তথ্য বিনিময় ঘটে।

একটি পিএসটিএন ধরনের পিওএস টার্মিনালের তুলনায় জিপিআরএস ধরনের পিওএস টার্মিনালের বেশি সুবিধা রয়েছে। একটি জিপিআরএস ধরনের পিওএস টার্মিনাল যে কোনো জায়গায় সরানো যেতে পারে, কারণ এতে একটি সিম এবং বিল্ট-ইন ব্যাটারি রয়েছে।

### ৪.২. পিওএস টার্মিনালে সমর্থিত লেনদেনের ধরন

একজন মার্চেন্ট একটি পিওএস টার্মিনাল ব্যবহার করে নিম্নলিখিত লেনদেন করতে পারেন—

বিক্রয় : গ্রাহক তার অ্যাকাউন্ট থেকে পণ্যদ্রব্য বা পরিষেবার মূল্য পরিশোধ করতে পারেন।

ভয়েড : দিন শেষ হওয়ার আগে, মার্চেন্ট যে কোনো সেল বাতিল করে গ্রাহককে টাকা ফেরত দিতে পারেন।

ফেরত : দিন শেষ হওয়ার পর, মার্চেন্ট যে কোনো সেল বাতিল করে গ্রাহককে টাকা ফেরত দিতে পারেন।

প্রাক-অনুমোদন : মার্চেন্ট একটি নির্দিষ্ট সময়ের জন্য গ্রাহকের অ্যাকাউন্ট থেকে কিছু পরিমাণ অর্থ ব্লক করতে পারেন। এটি সাধারণত হোটেলগুলোতে ব্যবহৃত হয়। মার্চেন্ট সেবা প্রদানের বিপরীতে এটি অর্থ পেতে গ্যারান্টি দেয়।

নগদ টাকা প্রদান : গ্রাহকগণ তার অ্যাকাউন্ট থেকে টাকা পেতে পিওএস ব্যবহার করতে পারেন। ব্যবসায়ীরা পণ্য বা পরিষেবার পরিবর্তে গ্রাহকদের টাকা দেন। এটি এটিএম ব্যবহার করে অ্যাকাউন্ট থেকে টাকা ওঠানোর মতোন একটি বিষয়।

### ৪.৩. পিওএস স্পেসিফিকেশন

ব্র্যান্ড : পিওএস টার্মিনালের তিনটি জনপ্রিয় ব্র্যান্ড হলো—হাইপারকম, ভেরিফোন এবং ইনজেনিকো।

র‍্যাম : ২ এমবি থেকে ৮ এমবি ফ্ল্যাশ র‍্যাম

প্রসেসর : ARM ৩২ বিট/৩২ বিট RISC

ম্যাগনেটিক কার্ড রিডার : IOS ১/২/৩

স্মার্ট কার্ড রিডার : EMV লেভেল ১ এবং ২ এবং ISO ১/২/৩

এনক্রিপশন : ট্রিপল DES

প্রিন্টার : থার্মাল

প্রদর্শন : গ্রাফিক, ১২৮x৬৪ পিক্সেল; ব্যাকলাইট

যোগাযোগ : GPRS/PSTN

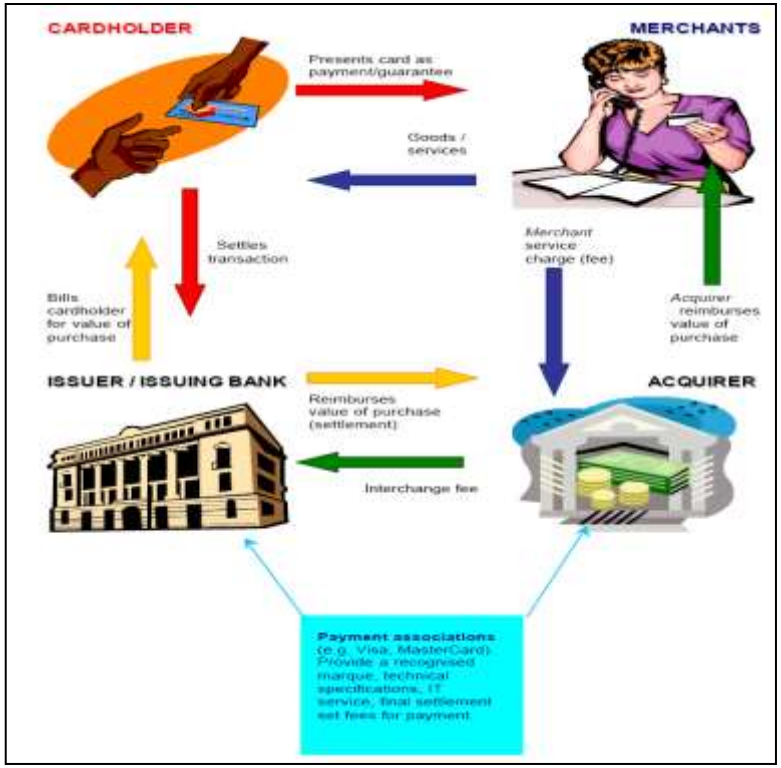
### ৪.৪. পিওএস কীভাবে কাজ করে?

পিওএস লেনদেন হলো একটি ক্রয় প্রক্রিয়া, যা একজন কার্ডধারীর মাধ্যমে শুরু হয়। নিচের চিত্রটি আমাদের লেনদেন প্রক্রিয়াটি আরও ভালোভাবে বুঝতে সাহায্য করবে। মূলত লেনদেন প্রক্রিয়াটি ক্রয়ের প্রক্রিয়ার একটি সিরিজ, যা কার্ডধারক থেকে শুরু হয়—

ক. কার্ডধারী ব্যবসায়ীর কাছ থেকে পণ্য বা পরিষেবা ক্রয় করেন।

খ. মার্চেন্ট, মূলত দ্রব্যটি Acquring ব্যাংকের কাছে বিক্রি করে বলে ধরে নেওয়া যায় এবং ডিসকাউন্ট ফি বাদে মূল্যের টাকা Acquring ব্যাংকের কাছ থেকে আদায় করে।

গ. অতপর অ্যাকুয়ারিং ব্যাংক লেনদেনের তথ্য সেন্ট্রাল ব্যাংক বা পেমেন্ট




*পিওএস টার্মিনাল কীভাবে কাজ করে*

অ্যাসোসিয়েশন (যেমন, ভিসা, মাস্টারকার্ড, ইত্যাদি) এর 'বিনিময় এবং নিষ্পত্তি ব্যবস্থার' মাধ্যমে ইস্যুয়িং ব্যাংকের কাছে উপস্থাপন করে।

ঘ. ইস্যুয়িং ব্যাংক ইন্টারচেইঞ্জ ফি বাদ দিয়ে দ্রব্যমূল্যের বাকি টাকা ব্যাংক বা পেমেন্ট অ্যাসোসিয়েশনের 'নিষ্পত্তি ব্যবস্থার মাধ্যমে' অ্যাকুয়ারিং ব্যাংকে প্রদান করে। ইন্টারচেইঞ্জ ফি ইস্যুয়িং ব্যাংকের খরচের আংশিক বহন করে।

ঙ. অবশেষে কার্ডধারী ক্রয়মূল্য ইস্যুয়িং ব্যাংকে পরিশোধ করে।

### ৪.৫. পিওএস পরিভাষা

ক. পিন প্যাড **(PIN Pad)**

কার্ডধারীর পিন গ্রহণ এবং তা এনক্রিপ্ট করার জন্য পিওএস টার্মিনালের সঙ্গে একটি পিন প্যাড থাকে। পিওএস টার্মিনালে ডেবিট কার্ডের মাধ্যমে লেনদেন গ্রহণ করতে, পিওএস টার্মিনালে একটি আলাদা বা বিল্ট-ইন পিন প্যাড থাকতে হয়।

খ. ইনচার্ট এবং সোয়াইপ করা **(Insert and Swipe)**

একটি নন-ইএমভি কার্ড পিওএস টার্মিনালে সোয়াইপ করতে হয়, কিন্তু EMV কার্ড পিওএস টার্মিনালে ইনচার্ট করতে হয়।

গ. মার্চেন্ট কমিশন **(Merchant Commission)**

ইহা বিক্রয় মূল্যের শতাংশে একটি কমিশন, যা ব্যবসায়ী POS টার্মিনাল সরবরাহকারী ব্যাংককে প্রদান করে। যদি একজন মার্চেন্ট ১০০ টাকা মূল্যে একটি আইটেম বিক্রি করে এবং কার্ডধারক তার কার্ড ব্যবহার করে বিল পরিশোধ করে এবং সম্মত মার্চেন্ট কমিশন ২% হয়, তাহলে ব্যাংক কার্ডধারীর কাছ থেকে ১০০ টাকা পায়, কিন্তু মার্চেন্টকে ৯৮ টাকা প্রদান করে।

**ঘ. বিনিময় ফি (Interchange fee)**

পিওএস-এর বিনিময় ফি হলো সেই ফি, যা অ্যাকুয়ারিং ব্যাংক ইস্যুয়িং ব্যাংককে প্রদান করে। যদি একটি ব্যাংকের কার্ডধারী তাহার কার্ড দিয়ে একটি মার্চেন্টের কাছে বিল পরিশোধ করে যেখানে অন্য ব্যাংক POS টি সরবরাহ করেছে, তখন ইন্টারচেঞ্জ ফি প্রদানের বিষয় আসে। ইন্টারচেঞ্জ ফি কেন্দ্রীয় ব্যাংক বা পেমেন্ট অ্যাসোসিয়েশন দ্বারা নির্ধারিত হয়। যেমন যদি মাস্টারকার্ডের জন্য ইন্টারচেঞ্জ ফি ১.১৬% হয় তাহলে উপরের উদাহরণে, অ্যাকুয়ারিং ব্যাংক ২.০% কমিশন উপার্জন করবে, কিন্তু কার্ডধারী অন্য ব্যাংকের হওয়ায় অ্যাকুয়ারিং ব্যাংক তার মার্চেন্ট কমিশন থেকে বিক্রয় মূল্যের ১.১৬% ইস্যুয়িং ব্যাংককে দিয়ে দেবে।

### ৪.৬. পিওএস এ প্রতারণা এবং প্রতিকার (Fraud at POS and remedy)

জালিয়াতরা তাদের জাল কার্ডগুলো সাধারণত ঐসব পণ্য ক্রয়ের বিপরীতে মার্চেন্টের POS টার্মিনালে ব্যবহার করে, যা তাহারা সহজেই বাজারে বিক্রি করতে পারে (যেমন সোনা ও ইলেকট্রনিক আইটেম)।

একটি জাল কার্ড হলো এমন একটি কার্ড, যা হয় আসল বা জাল কার্ড নম্বর ব্যবহার করে অপরাধীরা তৈরি করেছে বা একটি বৈধ কার্ড পরিবর্তন করে তা ব্যবহার করছে।

স্কিমিং-এর মাধ্যমে বেশিরভাগ জাল কার্ড জালিয়াতির সূত্রপাত হয়। এই প্রক্রিয়ার মাধ্যমে একটি বৈধ কার্ডের বিশদ তথ্যাবলি কার্ডের ম্যাগনেটিক স্ট্রিপ থেকে রেকর্ড করা হয় এবং পরবর্তীতে অপরাধীদের দ্বারা একটি জাল কার্ডে তা এনকোড করা হয়। স্কিমিং সাধারণত দোকানের কর্মীদের দ্বারা সংঘটিত হয় যারা কার্ডধারকের বৈধ কার্ড গ্রাহকের অগোচরে একটি পকেট-আকারের রেকর্ডিং ইউনিট ব্যবহার করে কার্ডের তথ্যাদি রেকর্ড করে থাকে। তারপরে তারা রেকর্ডকৃত তথ্য সংঘটিত অপরাধী গোষ্ঠীর কাছে বিক্রি করে, যারা পরবর্তীতে ঐ তথ্য ব্যবহার করে জাল কার্ড তৈরি করে। যাইহোক, স্কিমড ডেটার ব্যবহার করে জাল কার্ড তৈরি করে তা শুধু POS এই ব্যবহারের মধ্যে সীমাবদ্ধ নয়। এ ধরনের ডেটা বা তথ্য ব্যবহার করে ই-কমার্স লেনদেনের মাধ্যমেও প্রতারণামূলক কার্য্যকলাপ করে থাকে।

কার্ডের তথ্য হাতে পাওয়ার পরে, জালিয়াতরা একটি ব্যাংকের নাম, তার নিজের নাম, ছবি এবং স্বাক্ষরসহ একটি জাল কার্ড তৈরি করে। তবে মেগ-স্ট্রিপের ভেতরে, তিনি জালিয়াতির শিকার হওয়া ব্যক্তির কার্ডের তথ্য ব্যবহার করেন। কেনাকাটা করার পর যখন তিনি মার্চেন্টের কাছে কার্ডটি হস্তান্তর করেন, তখন ব্যবসায়ী দেখতে পান যে ছবি এবং স্বাক্ষর পুরোপুরি মিলে যাচ্ছে। কিন্তু, পিওএসের কাছে অন্য লোকের তথ্য যায়। পিওএস এই তথ্য অ্যাকুয়ারিং ব্যাংকের কাছে পাঠায়, অ্যাকুয়ারিং ব্যাংক তা প্রতারিত ব্যক্তির ব্যাংকে অর্থাৎ ইস্যুয়িং ব্যাংকে পাঠায়। ইস্যুকারী ব্যাংক সবকিছু ঠিকঠাক খুঁজে পায়, ফলে লেনদেন অনুমোদন করে। এভাবে মার্চেন্ট প্রতারকের হাতে বিক্রিত দ্রব্যাদি হস্তান্তর করে।

মার্চেন্ট পিওএস ব্যাচ বন্ধ করার পরে, অ্যাকুয়ারিং ব্যাংক থেকে তার অ্যাকাউন্টে তার অর্থ পেয়ে যাবে। অ্যাকুয়ারিং ব্যাংকও ইস্যুয়িং ব্যাংক থেকে অর্থ পাবে। কিন্তু যখন কার্ডধারী ইস্যুয়িং ব্যাংক থেকে বিল পাবেন, তখন তিনি এই অর্থ প্রদান করতে অস্বীকার করবেন কারণ তিনি এই লেনদেন করেননি।

তদন্ত শুরু হবে। এই দুই ব্যাংকের যে কোনো একটিকে লোকসান গ্রহণ করতে হবে। তাদের মধ্যে যেটি EMV কমপ্লায়েন্ট হবে সেটি জয়ী হবে। উভয় ব্যাংকই যদি নন-ইএমভি হয়, তাহলে কে ক্ষতি বহন করবে? সেই সিদ্ধান্ত পেমেন্ট অ্যাসোসিয়েশন গ্রহন করবে। যদি উভয় ব্যাংকই ইএমভি কমপ্লায়েন্ট হয় তখন এমন প্রতারণা হওয়ার সুযোগ নেই।

তাই, কার্ড জালিয়াতি থেকে বাঁচাতে গ্রাহক, মার্চেন্ট, ব্যাংক এবং পেমেন্ট অ্যাসোসিয়েশনগুলোকে কিছু সতর্কতা অবলম্বন করতে হবে যাহা এই মডিউলে '৫.৭. কার্ড জালিয়াতি প্রতিরোধ কৌশল' শিরোনামে বর্ণিত হয়েছে।

## ৫. ডেবিট কার্ড, ক্রেডিট কার্ড, কার্ড প্রযুক্তি, এবং কার্ড জালিয়াতি

আজকাল কার্ড ব্যবহার না করে আধুনিক ব্যাংক অপারেশন, বাণিজ্যিক লেনদেন এবং বিভিন্ন ধরনের পেমেন্ট কল্পনা করা প্রায় অসম্ভব। নির্ভরযোগ্যতা, সর্বজনীনতা ও সুবিধার কারণে কার্ডগুলো সারা বিশ্বে সমাদৃত হয়েছে এবং ব্যাপক প্রচলন পেয়েছে। সুতরাং বর্তমানে ভিসা কার্ডধারীদের সংখ্যা ৩০০ মিলিয়নেরও বেশি দাঁড়িয়েছে। এছাড়াও মাস্টারকার্ড, আমেরিকান এক্সপ্রেস (এমএক্স), ডিনারস ক্লাব (ডিসি), জেসিবি এবং অসংখ্য জাতীয়, আঞ্চলিক এবং স্থানীয় (আন্তঃ- এবং মনো-ব্যাংক) কার্ড এসোসিয়েশন মিলে আরও ৩০০ মিলিয়ন কার্ডের গ্রাহক তৈরি করেছে। যুক্তরাজ্য এবং মার্কিন যুক্তরাষ্ট্রে প্রায় ৯০% প্রাপ্তবয়স্কদের এক বা একাধিক কার্ড রয়েছে।

গত কয়েক বছরে বাংলাদেশে আর্থিক পরিষেবার ক্ষেত্রে, ডাচ্-বাংলা ব্যাংকের নেক্সাস কার্ড ও বিভিন্ন ব্যাংক কর্তৃক বিতরণকৃত ভিসা ও মাস্টারকার্ড ছাড়াও রয়েছে 'কিউ-ক্যাশ' এর মতো একটি নতুন ধরনের পেমেন্ট সিস্টেম।

### ৫.১. কার্ডের ধরন

বিভিন্ন ধরনের কার্ড রয়েছে। সর্বাধিক জনপ্রিয় কার্ডগুলো নিচে তালিকাভুক্ত করা হলো—

ক. ক্রেডিট কার্ড

ব্যাংক গ্রাহকের ক্রেডিট সীমা মূল্যায়ন করে গ্রাহকের সঙ্গে একটি চুক্তি স্বাক্ষর করে এবং গ্রাহককে ক্রেডিট কার্ড প্রদান করে। গ্রাহক ঐ ক্রেডিট সীমা পর্যন্ত মূল্যের পন্য ও সেবা ঐ কার্ড দিয়ে পেমেন্ট করতে পারেন। অতঃপর তিনি একটি নির্দিষ্ট গ্রেস পিরিয়ডের মধ্যে (বিলিং তারিখ থেকে ৪০-৫০ দিন) কোনো সুদ ছাড়াই সম্পূর্ণ অর্থ প্রদান করে থাকেন। বেশিরভাগ ক্রেডিট কার্ড ইস্যুকারী ব্যাংকের একটি ন্যূনতম পেমেন্ট সীমা থাকে যা সাধারণত টাকা ৫০০/- বা ৫-১০% এর মধ্যে যেটি বেশি তা হয়। গ্রাহক গ্রেস পিরিয়ডের মধ্যে ন্যূনতম বা তার চেয়ে বেশি বা

সম্পূর্ণ পরিমাণ অর্থ প্রদান করতে পারেন। যদি গ্রাহক আংশিক অর্থ প্রদান করেন, তাহলে ব্যাংক প্রতি মাসে বকেয়া ঋণের ওপর সুদ গ্রহণ করে থাকে।

গ্রাহকের কাছে একটি মাসিক স্টেটমেন্ট পাঠানো হয় যাতে তার অ্যাকাউন্টের বিশদ বিবরণ, সে কী খরচ করেছে, কোথায়, কোন তারিখে এবং তার কাছে কত টাকা পাওনা রয়েছে ইত্যাদি উল্লেখ করা থাকে। গ্রাহক সম্পূর্ণ অর্থ পরিশোধ করলে তাকে কোনো সুদ দিতে হয় না। কিন্তু তিনি যদি আংশিক অর্থ পরিশোধ করেন, তখন তাকে বাকি টাকার ওপর সুদ দিতে হবে। একটি ক্রেডিট কার্ড সাধারণত পিওএস টার্মিনালে ব্যবহার করা হয়, তবে টাকা তোলার জন্য তাহা এটিএম-এ ব্যবহার করা যেতে পারে। এ ক্ষেত্রে টাকা তোলার দিন থেকে গ্রাহককে নগদ টাকা তোলার পরিমাণের উপর সুদ দিতে হবে। ক্রেডিট কার্ড প্রদানকারী ব্যাংক সিগনেচার, ওয়ার্ল্ড, প্ল্যাটিনাম, টাইটানিয়াম, গোল্ড বা সিলভার জাতীয় ক্রেডিট কার্ড গ্রাহককে দিয়ে থাকে। সব ক্রেডিট কার্ডই ঋণ সুবিধা দিয়ে থাকে, কিন্তু প্রতিটি কার্ডের রয়েছে বিভিন্ন শর্ত এবং সুবিধা।

**খ. ডেবিট কার্ড**

এই কার্ডগুলো নগদ টাকা ব্যবহার বা চেক লেখার বিকল্প হিসাবে কাজ করে। ডেবিট কার্ড ব্যবহার করলে টাকা সরাসরি গ্রাহকের ব্যাংক অ্যাকাউন্ট থেকে কেটে নেওয়া হয়। কার্ডটি এটিএম মেশিনে ব্যবহার করে গ্রাহক তার নিজ অ্যাকাউন্ট থেকে নগদ টাকা তুলতে পারেন এবং এটি POS টার্মিনালে ব্যবহার করে পণ্য ও পরিষেবার মূল্য প্রদান করতে পারেন। ডেবিট কার্ড পাওয়ার শর্ত হলো, গ্রাহকের অবশ্যই একটি অ্যাকাউন্ট থাকতে হবে।

**গ. প্রি-পেইড কার্ড**

প্রি-পেইড কার্ড পাওয়ার জন্য ব্যাংকে অ্যাকাউন্ট থাকার প্রয়োজন নেই। গ্রাহক প্রথমে তার প্রি-পেইড কার্ডে টাকা লোড করে নেন। পরে তিনি তা নগদ টাকার বিকল্প হিসাবে এটিএম, পিওএস বা ই-কমার্স সাইটে ব্যবহার করে থাকেন।

**ঘ. এটিএম কার্ড**

এগুলো ক্যাশ কার্ড, ক্যাশ ডিসপেনসার কার্ড বা ক্যাশ মেশিন কার্ড নামেও পরিচিত। এই কার্ডটি এটিএম-এ নগদ তোলা এবং অন্যান্য ব্যাংকিং পরিষেবার জন্য ব্যবহার করা হয়। এটিএম কার্ড পিওএস-এ ব্যবহার করা যায় না।

## ৫.২. এটিএম এবং পিওএস টার্মিনালে কার্ড লেনদেনের পরিভাষা

### ৫.২.১. ইস্যুয়ার এবং অ্যাকুয়ারার (Issuer and Acquierer)

যে ব্যাংক বা প্রতিষ্ঠান কার্ড ইস্যু করে তাকে ইস্যুয়ার বলে। আপনি যদি ডিবিবিএল থেকে ক্রেডিট/ডেবিট কার্ড নিয়ে থাকেন, তাহলে আপনার ইস্যুয়ার ব্যাংক হলো ডিবিবিএল।

যে ব্যাংক বা পেমেন্ট সংস্থাগুলো মার্চেন্ট অবস্থানে এটিএম বা পিওএস টার্মিনাল ইনস্টল করে তাদের বলা হয় অ্যাকুয়ারার। আপনি যদি ব্র্যাক ব্যাংকের এটিএম-এ ডিবিবিএল-এর একটি কার্ড ব্যবহার করেন, তাহলে এই ক্ষেত্রে অ্যাকুয়ারার ব্যাংকটি হবে ব্র্যাক ব্যাংক। আপনি যদি এটিএম-এ ১০,০০০ টাকা চেয়ে থাকেন, কিন্তু এটিএম আপনাকে কম টাকা প্রদান করেছে অথচ আপনার অ্যাকাউন্ট থেকে পুরো টাকাই ডেবিট হয়ে গেছে, সেই ক্ষেত্রে আপনাকে আপনার ইস্যুয়িং ব্যাংকের কাছে অভিযোগ করতে হবে, অ্যাকুয়ারিং ব্যাংকের কাছে নয়।

### ৫.২.২. অন-আস লেনদেন (On-us Transaction)

যদি কোনো লেনদেনের ক্ষেত্রে ইস্যুয়িং ও অ্যাকুয়ারিং ব্যাংকগুলো একই হয়, তবে লেনদেনটিকে অন-আস লেনদেন বলা হয়। উদাহরণস্বরূপ, যদি ব্যাংক-এ এর একজন গ্রাহক একই ব্যাংকের (ব্যাংক-এ) এটিএম/পিওএস-এ লেনদেন করেন, তাহলে সেই লেনদেনটিকে অন-আস লেনদেন বলা হয়।

### ৫.২.৩. অফ-আস বা নট অন-আস লেনদেন (Off-us and not-on-us Transaction)

যদি অন্য ব্যাংকের কোনো গ্রাহক আমাদের ব্যাংকের এটিএম/পিওএস-এ লেনদেন করেন, তাহলে লেনদেনকে অফ-আস বা নট অন-আস বলা হয়। উদাহরণস্বরূপ, যদি ব্যাংক-বি-এর কোনো গ্রাহক ব্যাংক-এ-এর এটিএম/পিওএস-এ লেনদেন করেন, তাহলে লেনদেনটিকে ব্যাংক-এ-এর ক্ষেত্রে অফ-আস বা নট অন-আস বলা হয়। কিন্তু এই লেনদেনকে ব্যাংক-বি-তে রিমোট অন-আস হিসাবে আখ্যায়িত করা হবে।

### ৫.২.৪. রিমোট অন-আস লেনদেন (Remote on-us Transaction)

আমাদের ব্যাংকের কোনো গ্রাহক যদি অন্য ব্যাংকের এটিএম/পিওএস-এ লেনদেনরেন, তাহলে সেই লেনদেনকে আমাদের ব্যাংকে রিমোট অন-আস বলে।

উদাহরণস্বরূপ, যদি ব্যাংক-এ এর একজন গ্রাহক ব্যাংক-বি-এর এটিএম/পিওএস-এ লেনদেন করেন, তাহলে সেই লেনদেনটিকে ব্যাংক-এ-তে রিমোট অন-আস

হিসাবে আখ্যায়িত করা হয়। কিন্তু এই লেনদেনটি ব্যাংক-বি-তে অফ-আস বা নট অন-আস হিসাবে বলা হবে।

### ৫.২.৫. ইন্টারচেঞ্জ ফি (Interchange fee)

যদি ব্যাংক-এ-এর কোনো গ্রাহক ব্যাংক-বি-এর এটিএম-এ লেনদেন করেন, তাহলে ব্যাংক-এ ব্যাংক-বি-কে একটি চার্জ প্রদান করবে। ব্যাংক-এ গ্রাহকদের কাছ থেকে এই ধরনের চার্জ (সাধারণত এই পরিমাণের বেশি) আদায় করবে এবং নির্ধারিত পরিমাণ চার্জ ব্যাংক-বি-কে দেবে।

অন্যদিকে, যদি ব্যাংক-এ-এর কোনো গ্রাহক ব্যাংক-বি-এর পিওএস-এ লেনদেন করেন, তাহলে ব্যাংক-বি ব্যাংক-এ-কে চার্জ দেবে। ব্যাংক-বি পিওএস মার্চেন্টের বিক্রয় লব্ধ আয় থেকে এই চার্জ আদায় করবে, যাকে মার্চেন্ট কমিশন বলা হয়।

এক ব্যাংক অন্য ব্যাংকে প্রদেয় উপরোক্ত চার্জগুলোকে ইন্টারচেঞ্জ ফি বলে। ইন্টারচেঞ্জ ফি মাস্টারকার্ড, ভিসা, ডাইনার ক্লাব, ডিসকভার এবং জেবিসি এর মতো আন্তর্জাতিক পেমেন্ট অ্যাসোসিয়েশন দ্বারা নির্ধারিত হয় এবং স্থানীয় এবং আন্তর্জাতিক কার্ড, EMV এবং নন-ইএমভি কার্ড, বা কার্ডের ধরন (সিগনেচার, প্ল্যাটিনাম বা গোল্ড কার্ড) এর জন্য আলাদা হতে পারে বা লেনদেনের ধরন (ইউটিলিটি বিল বা মার্চেন্ট পেমেন্ট) অনুযায়ীও আলাদা হতে পারে। ইন্টারচেঞ্জ ফি কেন্দ্রীয় ব্যাংক দ্বারাও নির্ধারিত হতে পারে।

### ৫.২.৬. মার্চেন্ট কমিশন (Merchant Commission)

ব্যাংক মার্চেন্টদের (দোকান, হোটেল, ইত্যাদি) বিনামূল্যে পিওএস টার্মিনাল প্রদান করে। ব্যাংক পিওএস টার্মিনালের জন্য প্রয়োজনীয় কাগজপত্র সরবরাহ করে এবং নিয়মিত রক্ষণাবেক্ষণ করে। বিনিময়ে, ব্যাংক মার্চেন্টের বিক্রয় আয় থেকে একটি কমিশন পায়। এই কমিশনকে মার্চেন্ট কমিশন বলা হয়। মার্চেন্ট কমিশন মার্চেন্টভেদে (মার্চেন্টের মোট বিক্রির পরিমাণের ওপর ভিত্তি করে) পরিবর্তিত হয়, যা ব্র্যান্ডেড কার্ডের জন্য ১.৫০% থেকে ৩.০০% এবং প্রপ্রাইটারি কার্ডের জন্য ১.০০% থেকে ২.০০% পর্যন্ত হয়ে থাকে।

### ৫.২.৭. ইএমভি এবং চিপ কার্ড (EMV and Chip card)

প্রচলিত কার্ডগুলোতে কার্ডের পিছনে ম্যাগনেটিক স্ট্রিপ থাকে, যা গ্রাহক এবং কার্ড সম্পর্কিত তথ্য সংরক্ষণ করে। ম্যাগনেটিক স্ট্রিপ থেকে তথ্য পুনরুদ্ধার করা সহজ। যখন কার্ডটি মার্চেন্টের কাছে লেনদেনের জন্য হস্তান্তর করা হয় বা এটিএম-এ ব্যবহার করা হয়, হ্যাকাররা সহজেই ম্যাগনেটিক স্ট্রিপের ভেতরের তথ্য কপি করতে পারে এবং তা দিয়া একটি ডুপ্লিকেট কার্ড তৈরি করতে পারে। এই ডুপ্লিকেট কার্ড ব্যবহার করে, তারা POS বা এটিএম-এ (যদি পিনও সংগ্রহ করা


*ইভিএম কার্ড*

যায়, যা মেগ-স্ট্রিপে সংরক্ষণ করা হয় না) লেনদেন করে থাকে। এ ধরনের প্রতারণামূলক কর্মকাণ্ড দিন দিন বেড়েই চলেছে। এটি রক্ষা করার জন্য, ইউরোপে, মাস্টারকার্ড এবং ভিসা যৌথভাবে EMV নামে একটি নিরাপত্তা ব্যবস্থা তৈরি করেছে। EMV মানে ইউরোপে-মাস্টারকার্ড-ভিসা। কিছু কম্পিউটার অ্যালগরিদম ব্যবহার করে ইএমভি কার্ডের কম্পিউটার চিপে তথ্য সংরক্ষণ করা হয়, যা কপি করা এবং পুনরুদ্ধার করা খুব কঠিন। একটি সাধারণ চিপ কার্ড এবং একটি ইএমভি চিপ কার্ড, উভয়ই কম্পিউটার চিপ ব্যবহার করে, তবে ইএমভি কার্ডে, ইউপে, মাস্টারকার্ড এবং ভিসা দ্বারা নির্ধারিত এবং প্রত্যয়িত কিছু কম্পিউটার যুক্তি রয়েছে। ফলে ইএমভি কার্ড বিশ্বের সবচেয়ে নিরাপদ কার্ড। ইউপে নামক পেমেন্ট অ্যাসোসিয়েশনটিকে মাস্টারকার্ড কিনে নিয়েছে।

### ৫.২.৮. লায়াবিলিটি সিফ্‌টিং (Liability Shifting)

ইএমভি লায়াবিলিটি সিফ্‌টিং নামে একটি নিয়ম ঘোষণা করেছে। এই নিয়ম অনুযায়ী, যদি কোনো জালিয়াতি ঘটে থাকে, তাহলে নন-ইএমভি পার্টি সবসময় জালিয়াতির জন্য দায়ী থাকবে। ফলে নন-ইএমভি পার্টিকে জালিয়াতির টাকা ইএমভি পার্টিকে দিতে হবে। এভাবে যদি একজন গ্রাহক বিশ্বের যে কোনো জায়গায় একটি EMV কার্ড ব্যবহার করেন এবং যদি তার কার্ড নম্বর ব্যবহার করে কোনো Non-EMV এটিএম বা পিওএস টার্মিনালে জালিয়াতি ঘটে, তাহলে গ্রাহক এবং তার ইস্যুয়িং ব্যাংক সর্বদা নিরাপদ থাকে।

যদি এটিএম এবং পিওএস ইএমভি প্রত্যয়িত হয়, তবে মাস্টারকার্ড এবং ভিসার ইএমভি প্রযুক্তি গ্যারান্টি দেয় যে এই টার্মিনালগুলোতে জাল কার্ড গ্রহণ করা হবে না, কারণ এই টার্মিনালগুলো কখনই কোনো ইএমভি কার্ডের মেগ-স্ট্রিপ অংশ

পড়বে না। যদি এটিএম এবং পিওএস টার্মিনালগুলো ইএমভি প্রত্যয়িত না হয়, তবে তারা চিপ পড়তে সক্ষম হবে না, বরং একটি এএমভি কার্ডের মেগ-স্ট্রিপ অংশ পড়তে পারবে।

### ৫.২.৯. চার্জ ব্যাক (Charge Back)

যদি ব্যাংক-বি-এর পিওএস/এটিএম টার্মিনালে ব্যাংক-এ এর কার্ড ব্যবহার করে জালিয়াতি ঘটে, তবে ব্যাংক-এ এর গ্রাহকের ব্যাংক অ্যাকাউন্ট বা ক্রেডিট কার্ড অ্যাকাউন্ট ডেবিট করা হয়েছে। এইভাবে গ্রাহক যখন তার অ্যাকাউন্টের স্টেইটম্যান্ট পাবেন, তখন তিনি দেখতে পাবেন যে কিছু লেনদেন তার স্টেইটম্যান্টে প্রতিফলিত হয়েছে যা তার নিজের দ্বারা করা হয়নি। তারপরে, তিনি তার ইস্যুয়ারকে (ব্যাংক) এটি রিপোর্ট করবেন। ইস্যুয়ার লেনদেনটি বিশ্লেষণ করবে এবং যদি দেখে যে পেমেন্ট অ্যাসোসিয়েশনের নিয়ম অনুযায়ী তাদের অ্যাকুয়ারিং ব্যাংক থেকে টাকা ফেরত পাওয়ার অধিকার আছে, তাহলে তারা পেমেন্ট অ্যাসোসিয়েশনের মাধ্যমে তাদের নস্ট্রো অ্যাকাউন্টে টাকা ফিরিয়ে আনবে। টাকা ফেরত আনার এই প্রক্রিয়াকে বলা হয় চার্জ-ব্যাক।

## ৫.৩. আন্তর্জাতিক পেমেন্ট অ্যাসোসিয়েশন

প্লাস্টিক মানি পেমেন্ট অ্যাসোসিয়েশন/সিস্টেম বা কার্ড অ্যাসোসিয়েশন দ্বারা শ্রেণিকরণ করা যেতে পারে। সবচেয়ে বিখ্যাত পেমেন্ট অ্যাসোসিয়েশন/সিস্টেম হল মাস্টারকার্ড, ভিসা, অ্যামেক্স, জেবিসি, ডাইনার ক্লাব, ডিসকভার এবং ইউনিয়ন পে অব চায়না। একটি কার্ড শুধু একটি পেমেন্ট সিস্টেম দ্বারা সমর্থিত এবং শুধু ঐ পেমেন্ট সিস্টেমের সেবাসমূহ প্রদান করতে পারে।

কিছু পেমেন্ট অ্যাসোসিয়েশন/সিস্টেম শুধু কয়েক ধরনের কার্ড সরবরাহ করতে পারে। উদাহরণস্বরূপ, আমেরিকান এক্সপ্রেস এবং ডিনারস ক্লাব শুধু ক্রেডিট কার্ড সরবরাহ করে এবং অন্যরা শুধু ডেবিট কার্ড প্রদান করতে পারে। ভিসা ও মাস্টারকার্ড-এর মতো বিশ্ব-বিখ্যাত পেমেন্ট অ্যাসোসিয়েশন উভয় ধরনের কার্ডই প্রদান এবং সমর্থন করে।

বিভিন্ন সিস্টেমের ক্রেডিট কার্ড বিভিন্ন শ্রেণিতে বিভক্ত। ভিসার চারটি প্রধান শ্রেণি রয়েছে: ক্লাসিক, গোল্ড, প্লাটিনাম ও সিগনেচার। মাস্টারকার্ডের ক্লাস আছে: স্ট্যান্ডার্ড, গোল্ড, টাইটানিয়াম ও ওয়ার্ল্ড।

### ৫.৩.১. মাস্টারকার্ড (Master card)

মাস্টারকার্ডের গল্পটি ১৯৬৬ সালে শুরু হয় যখন ব্যাংকগুলোর একটি গ্রুপ একটি সদস্য-ভিত্তিক সমিতি তৈরি করে যা পরে মাস্টারকার্ডে পরিণত হয়। ১৯৬৮ সালে কোম্পানিটি মেক্সিকো, জাপান এবং ইউরোপে তার উপস্থিতি প্রসারিত করে, যা





শীর্ষস্থানীয় বিশ্বব্যাপী অর্থপ্রদানের নেটওয়ার্ক হওয়ার প্রতিশ্রুতির সূচনা করে। ১৯৮০-এর দশকে, মাস্টারকার্ড এই প্রতিশ্রুতির ওপর ভিত্তি করে চলা অব্যাহত রাখে এবং বিশ্বজুড়ে নতুন অঞ্চল ও বাজারে ইলেকট্রনিক পেমেন্টের সুবিধা নিয়ে আসে।

মাস্টারকার্ড ২০০২ সালে ইউরোপে ইন্টারন্যাশনালের সঙ্গে একীভূত হয়, একটি ইউনিফাইড গ্লোবাল কর্পোরেট কাঠামো প্রতিষ্ঠা করে এবং একটি কর্পোরেশনে পরিণত হয়।

গ্লোবাল হেডকোয়ার্টার : পার্চেজ, নিউইয়র্ক

কর্মচারী :

২০১০ সালের হিসাবে আনুমানিক ৫১০০ (বিশ্বজুড়ে বিভিন্ন অফিসে অবস্থিত)।

বিশ্বব্যাপী পরিধি বা সীমা—

মাস্টারকার্ড ভৌগোলিকভাবে নিম্নলিখিত অঞ্চলে সংগঠিত—এশিয়া প্যাসিফিক, মধ্যপ্রাচ্য, আফ্রিকা, কানাডা, ইউরোপ, লাতিন আমেরিকা এবং মার্কিন যুক্তরাষ্ট্র।

মাস্টারকার্ড বিশ্বব্যাপী ব্র্যান্ড :

মাস্টারকার্ড হলো বিশ্বের সর্বাধিক স্বীকৃত ক্রেডিট এবং ডেবিট কার্ড ব্র্যান্ডগুলোর মধ্যে একটি, যা তাৎক্ষণিক ক্রয়ক্ষমতা, তাৎক্ষণিক আমানত অ্যাক্সেস সুবিধা, বিশ্বব্যাপী নিরাপত্তা এবং নমনীয় অর্থপ্রদানের বিকল্পগুলোর প্রতিনিধিত্ব করে।

মায়েস্ট্রো হলো সর্বাধিক স্বীকৃত বিশ্বব্যাপী ডেবিট কার্ডগুলোর মধ্যে একটি। এটি একমাত্র অনলাইন, পিন-ভিত্তিক ডেবিট ব্র্যান্ড, যা বিশ্বব্যাপী এটিএম থেকে টাকা পেতে ও POS টার্মিনাল ব্যবহার করে কেনাকাটা করতে সাহায্য করে।


*মাস্টারকার্ডের একটি ক্রেডিট কার্ড (মাস্টারকার্ড) এবং একটি ডেবিট কার্ড (মায়েস্ট্রো)*

সিরাস হলো একটি ব্র্যান্ডের নাম, যা বিশ্বব্যাপী মাস্টারকার্ডের এটিএম নেটওয়ার্ককে বোঝায়, যা বিশ্বের বৃহত্তম এটিএম নেটওয়ার্কগুলোর মধ্যে একটি। সিরাস ব্র্যান্ড বিশ্বব্যাপী এক মিলিয়নেরও ATM-এর মাধ্যমে আমানতকারীদের অ্যাকাউন্ট অ্যাক্সেস সুবিধা দিয়ে থাকে।

সদস্যপদ :
মাস্টারকার্ড তাদের গ্রাহক হিসাবে হাজার হাজার আর্থিক প্রতিষ্ঠানের মাধ্যমে তাদের ব্র্যান্ড ও পণ্য বাজারজাত করে থাকে। এই সব ব্র্যান্ডের মধ্যে রয়েছে মাস্টারকার্ড, মায়েস্ট্রো, সিরাস, মাস্টারকার্ড ডেবিট এবং মাস্টারকার্ড পেপাশ।

মাস্টারকার্ড দুই ধরনের সদস্যপদ প্রদান কওে : প্রিন্সিপাল সদস্য এবং অ্যাসোসিয়েট সদস্য। প্রিন্সিপাল সদস্য হলো একটি সরাসরি সদস্য এবং এটি একটি এমআইপি (মাস্টারকার্ড ইন্টারফেস পয়েন্ট) ব্যবহার করে মাস্টারকার্ড নেটওয়ার্কের সঙ্গে সরাসরি সংযোগ থাকে। এই এমআইপি সদস্য ব্যাংকের ডেটা সেন্টারে স্থাপন করা হয়। অ্যাসোসিয়েট সদস্যের এমআইপি সেট আপ করার প্রয়োজন নেই, ফলে এটি একটি প্রিন্সিপাল সদস্যের মাধ্যমে সমস্ত লেনদেন রুট করে থাকে। সহযোগী সদস্যকে অপেক্ষাকৃত কম সদস্য ফি এবং অন্যান্য চার্জ দিতে হয়।

### ৫.৩.২. ভিসা (Visa)

ভিসা হলো একটি বিশ্বব্যাপী পেমেন্ট প্রযুক্তি কোম্পানি, যা বিশ্বব্যাপী ২০০টিরও বেশি দেশ ও অঞ্চলে গ্রাহক, ব্যবসা, ব্যাংক এবং সরকারকে সংযুক্ত করেছে। ভিসা ইনকর্পোরেটেডের সদর দপ্তর সান ফ্রান্সিসকোতে। ২০১০ সাল পর্যন্ত সারা বিশ্বে ভিসার প্রায় ৫,৫০০ কর্মী রয়েছে। তারা দুটি মহাদেশে তিনটি ডেটা সেন্টার পরিচালনা করে। ভিসা-ইউরোপ একটি পৃথক সদস্যপদ প্রদানকারী সংস্থা, যা ইউরোপীয় অঞ্চলে ভিসা ইনকর্পোরেটেডের ট্রেডমার্ক এবং প্রযুক্তির লাইসেন্স প্রদান করে থাকে।

ভিসা নেটওয়ার্কের বিস্তৃত :

- ১৫,৯০০ আর্থিক প্রতিষ্ঠান এর গ্রাহক
- ১.৭ মিলিয়ন এটিএম (৩১ মার্চ, ২০১০ অনুযায়ী)
- ২০০টি দেশ এবং অঞ্চল
- ১.৮ বিলিয়ন ভিসা কার্ড (মার্চ ৩১, ২০১০ অনুযায়ী)

**ভিসা প্রডাক্ট**

**ক্রেডিট প্রডাক্ট**

ভিসা বিভিন্ন ধরনের ক্রেডিট কার্ড অফার করে, যেমন—ভিসা প্লাটিনাম, ভিসা সিগনেচার এবং ভিসা ইনফিনিট। সমস্ত ভিসা ক্রেডিট কার্ড স্ট্যান্ডার্ড সুবিধা এবং বৈশিষ্ট্যসহ আসে, যার মধ্যে রয়েছে অটো রেন্টাল কলিসন ড্যামেজ ওয়েভার, ইমার্জেন্সি কার্ড রিপ্লেসমেন্ট এবং জিরো লায়াবিলিটি সুরক্ষা, যা অননুমোদিত কেনাকাটার ক্ষেত্রে কার্ডধারীদের রক্ষা করে।

**ডেবিট প্রডাক্ট**

ভিসা ডেবিট কার্ড যেমন ভিসা ইলেক্ট্রন এবং ভিসা ডেবিট নগদ টাকা বহনের চেয়ে নিরাপদ এবং চেক লেখার চেয়ে বেশি সুবিধাজনক। ভিসা ডেবিট কার্ড নিরাপত্তা সুরক্ষা প্রদান করে, যা জালিয়াতি প্রতিরোধ, শনাক্তকরণ এবং সমাধান করতে সাহায্য করে, যার মধ্যে ক্রমাগত জালিয়াতি নিরীক্ষণ এবং ভিসার জিরো দায় নীতি দ্বারা কভারেজ প্রাপ্ত। ইহা কার্ডধারীদের অননুমোদিত চার্জ থেকে রক্ষা করে।

**প্রি-পেইড প্রডাক্ট**

ভিসা বিভিন্ন খুচরা বিক্রেতা, আর্থিক প্রতিষ্ঠানের শাখা অফিস, নিয়োগকর্তা এবং সরকারি সংস্থাগুলোর মাধ্যমে ভিসা প্রিপেইড কার্ড এবং পরিষেবাগুলো প্রদান করে থাকে। এসব প্রিপেইড কার্ডের মধ্যে রয়েছে—


*ভিসার একটি ক্রেডিট কার্ড (ভিসা) এবং একটি ডেবিট কার্ড (ভিসা ইলেকট্রন)*

- ভিসা রিলোডযোগ্য প্রিপেইড কার্ড
- ভিসা গিফ্ট কার্ড

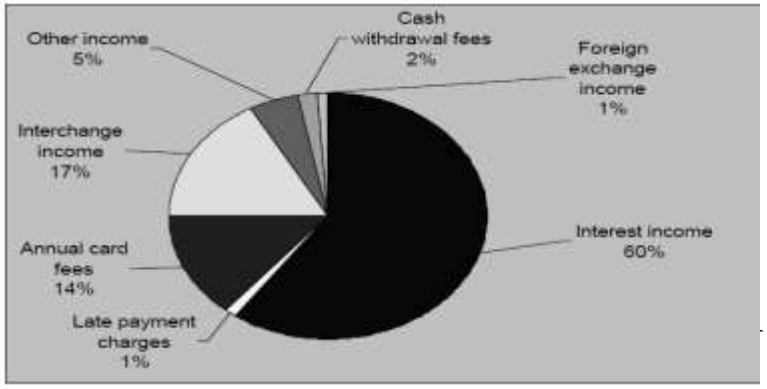
- ভিসা ট্রাভেলমানি কার্ড
- ভিসা হেলথ কেয়ার কার্ড
- ভিসা পেরোল কার্ড
- ভিসা ইনসেনটিভ কার্ড
- ভিসা সরকারি বিতরণ কার্ড
- ভিসা রেডিলিঙ্ক

**৫.৪. ক্রেডিট কার্ড ব্যবসা থেকে আয়**

ইস্যুকারী এবং অধিগ্রহণকারীর জন্য বিভিন্ন ধরনের আয় রয়েছে যেমন সুদের আয়, বার্ষিক কার্ড ফি, ইন্টারচেঞ্জ ফি, নগদ উত্তোলনের ফি, বিলম্বে পেমেন্ট চার্জ, বৈদেশিক মুদ্রা বিনিময় আয় ইত্যাদি, যা নিম্নলিখিত চার্ট থেকে দেখা যেতে পারে—

**৫.৪.১. ডেবিট কার্ড ইস্যু করা থেকে আয়ের উৎস (কার্ডধারীর দ্বারা প্রদেয়)**

১. কার্ড ইস্যু ফি
২. বার্ষিক/নবায়ন ফি
৩. কার্ড প্রতিস্থাপন ফি
৪. পিন রি-ইস্যু ফি
৫. ডেবিট কার্ড ইস্যুকারী হিসাবে, ব্যাংকের স্বল্প-মূল্যের আমানত বাড়ে যা পরোক্ষভাবে ব্যাংকের আয় বৃদ্ধিতে অবদান রাখে।




*ভিসা ইন্টারন্যাশনাল (২০০০)*

১. ইন্টারচেঞ্জ ফি (যদি অন্য ব্যাংকের কার্ড হোল্ডার এটিএম ব্যবহার করেন)
২. নগদ অগ্রিম ফি (যদি একজন ক্রেডিট কার্ডধারী এটিএম থেকে টাকা উত্তোলন করেন)
৩. কনজুমার কাগজ ফি (ATM লেনদেনের পর স্লিপ প্রদানের ফি)
৪. ভিডিও ফি (গ্রাহকের চাহিদা অনুযায়ী সিসিটিভি ভিডিও তাকে প্রদান করলে)

**৫.৪.৪. পিওএস অ্যাকুয়ারিং থেকে আয়ের উৎস (মার্চেন্ট/কার্ডধারীর দ্বারা প্রদেয়)**

১. বিক্রয় মূল্যের ওপর ১.৫০%-৩.০০% কমিশন (মার্চেন্ট দ্বারাপ্রদেয়)
২. বিদেশি লেনদেনের ক্ষেত্রে মুদ্রার বিনিময় উপার্জন (কার্ডধারীর কাছ থেকে কর্তনযোগ্য)

**৫.৫. কার্ড প্রযুক্তি**

**৫.৫.১. প্লাস্টিক (Plastic)**

প্লাস্টিক কার্ড হলো স্ট্যান্ডার্ড ডাইমেনশনের একটি প্লেট (৮৫.৬ মিমি x ৫৩.৯ মিমি x ০.৭৬ মিমি) যা তথ্য সংরক্ষণের জন্য ব্যবহৃত মেকানিক এবং থার্মো-প্রতিরোধী ধরনের বিশেষ প্লাস্টিক থেকে উৎপন্ন করা হয়।

**৫.৫.২. ম্যাগনেটিক স্ট্রিপ এবং মাইক্রো চিপ (Magnetic strip and Micro chip)**

ইলেকট্রনিক ডেটা মিডিয়া হিসাবে, কার্ডগুলোকে চৌম্বকীয় স্ট্রিপ কার্ড ও ইন্টিগ্রেটেড চিপ কার্ড (মাইক্রোপ্রসেসর কার্ড) এ ভাগ করা যায়। প্রথমগুলোকে ম্যাগনেটিক কার্ড বলা হয়, অন্যগুলোকে স্মার্ট কার্ড বা চিপ কার্ড বলা হয়।

একটি চৌম্বক স্ট্রিপ কার্ডের পেছনে একটি কালো রঙের ম্যাগনেটিক স্ট্রিপ থাকে। ISO 7811 স্ট্যান্ডার্ড অনুযায়ী ম্যাগনেটিক স্ট্রিপে তিনটি ট্র্যাক থাকে। তাদের মধ্যে প্রথম দুটি ট্র্যাকে শনাক্তকরণ ডেটা সংরক্ষণ করা হয় এবং তৃতীয়টি ট্র্যাকে অন্যান্য তথ্য লেখা হয় (উদাহরণস্বরূপ, একটি ডেবিট কার্ডের লিমিটের বর্তমান স্থিতি)। তবে রেকর্ডিং/পড়ার পুনরাবৃত্তি প্রক্রিয়া কম নির্ভরযোগ্য হওয়ার কারণে, ম্যাগনেটিক স্ট্রিপে রেকর্ডিং করা হয় না এবং এই জাতীয় কার্ডগুলো শুধু তথ্য পড়ার জন্য ব্যবহার করা হয়। এই ধরনের কার্ড প্রতারণার জন্য বেশ ঝুঁকিপূর্ণ। মার্কিন যুক্তরাষ্ট্রে ১৯৯২ সালে ম্যাগনেটিক স্ট্রিপসহ ক্রেডিট কার্ডের মাধ্যমে জালিয়াতির মোট ক্ষতি এক বিলিয়ন ডলার ছাড়িয়ে গেছে।

একটি ম্যাগনেটিক স্ট্রিপ কার্ডে, নিম্নলিখিত তথ্য ধারণ করা হয়—

ক. কার্ডের সামনের অংশে থাকে—

- কার্ডধারীর নাম।
- কার্ড নম্বর।
- কার্ডের মেয়াদ।
- কার্ড ইস্যুকারী ব্যাংকের লোগো।
- পেমেন্ট সিস্টেমের লোগো।
- কিছু কার্ডে অতিরিক্ত সুরক্ষার জন্য 'হলোগ্রাম' থাকে।

খ. কার্ডের পিছনের দিকে থাকে—

- কার্ডধারীর স্বাক্ষরের জন্য একটি জায়গা।
- ম্যাগনেটিক স্ট্রিপ।
- মালিকের ছবি (কিছু ক্ষেত্রে)।
- এটিএম নেটওয়ার্কের লোগো, যেখানে কার্ডধারী কার্ডের মাধ্যমে লেনদেন করতে পারেন।

কার্ড নম্বরটি ১৬টি সংখ্যা নিয়ে গঠিত—

- প্রথম ছয় সংখ্যা- ইস্যুয়িং ব্যাংকের কোড।
- পরবর্তী নয়টি নম্বর—কার্ডের ব্যাংক নম্বর (কার্ড অ্যাকাউন্ট নম্বর)।
- শেষের সংখ্যাটি নিয়ন্ত্রণ সংখ্যা।

স্মার্ট কার্ডগুলোতে, ডেটা ক্যারিয়ার হলো একটি মাইক্রোপ্রসেসর বা মাইক্রো-চিপ—যার মেমরি আকার ৩২ বাইট থেকে ১৬ কিলোবাইট পর্যন্ত হতে পারে। এই মেমোরিটি শুধু একবার রেকর্ডিং এবং বহুবার পড়া, অথবা বহুবার পড়া ও বহুবার রেকর্ডিং করা সাপোর্ট করে।

১৯৭০-এর দশকের গোড়ার দিকে স্মার্ট কার্ড আবিষ্কৃত হয়েছিল। ১৯৮০-এর দশকের মাঝামাঝি, ফরাসি ব্যাংকগুলো খুচরা লেনদেনের জন্য ডেবিট কার্ডে এই প্রযুক্তির ব্যাপক ব্যবহার শুরু করে।

মাইক্রোপ্রসেসর কার্ডের অপারেটিং সিস্টেমের মাধ্যমে মেমরি এবং পরিষেবা নিয়ন্ত্রণ এবং নিরাপত্তা ব্যবস্থার জন্য একাধিক ফাংশনসহ কার্ডে সংরক্ষিত ডেটার ওপর নির্দিষ্ট কিছু পদক্ষেপ নেওয়া সাপোর্ট করে।

স্মার্ট কার্ডে এম্বেড করা মাইক্রোচিপটি একটি সাধারণ মেমোরি-অনলি ডিভাইস (এটিকে ইন্টিগ্রেটেড সার্কিট বা আইসি কার্ডও বলা হয়) অথবা একটি জটিল রিড/রাইট মাইক্রোপ্রসেসর (এটিকে সেন্ট্রাল প্রক্রিয়াকরণ ইউনিট বা সিপিইউও বলা হয়) হতে পারে। সাধারণত, আজকাল আট কিলোবাইট স্টোরেজ ক্ষমতাসহ একটি চিপ পাওয়া যায়; এই পরিমাণ স্থানে ১,৬০০ শব্দের পাঠ্য বা ব্যবহারকারীর আঙুলের ছাপ, পাম প্রিন্ট বা রেটিনাল স্ক্যানের একটি ডিজিটাল চিত্র সংরক্ষণ করতে পারে। ১৬-কিলোবাইট চিপ ব্যাপকভাবে সহজলভ্য কিন্তু ৬৪-কিলোবাইট চিপও বাজারে পাওয়া যাচ্ছে।

এনক্রিপশন প্রযুক্তি অ্যাক্সেস কন্ট্রোল অ্যাপ্লিকেশনগুলোকে আরও সুরক্ষিত করে তোলে। কেউ তার রিডিং ডিভাইসকে এমনভাবে সেট আপ করতে পারে যাতে কার্ড এবং রিডারের মধ্যে সঠিকভাবে তথ্য সরবরাহ করার জন্য একটি ক্রিপ্টোগ্রাম ব্যবহার করা হয়। রিডার একটি নম্বর পাঠিয়ে কার্ডটিকে চ্যালেঞ্জ করবেন এবং কার্ডটিকে এটি এনক্রিপশন কী দিয়ে এনক্রিপ্ট করতে হবে এবং রিডারের কাছে ফেরত পাঠাতে হবে। রিডার এটি সঠিক কি না তা পরীক্ষা করে দেখে। শুধু একটি অথেনটিক কার্ডই জানবে কীভাবে এটি এনক্রিপ্ট করতে হয়। তাই সঠিক পাওয়া গেলে, অন্যান্য তথ্যের আদান-প্রদান শুধু করা হয়।

### ৫.৫.৩. ব্যাংক কার্ড পার্সোলাইজেশন (Personalization of bank card)

প্লাস্টিক কার্ডের ধরন এবং উদ্দেশ্যের ওপর নির্ভর করে, আপনি বিভিন্ন ধরনের পার্সোলাইজেশন পছন্দ করতে পারেন—

—চিপ-মডিউলের এনকোডিং

—ম্যাগনেটিক স্ট্রিপে রেকর্ডিং (হাইকো, লোকো)

—থার্মো প্রিন্টার বা বাবল জেটের মাধ্যমে স্ক্র্যাচ-স্ট্রিপ দিয়ে আবৃত অনন্য সংখ্যার (পিন, লগইন) ছাপ

—টিপিং দিয়ে এমবসিং

—বারকোডের ছাপ

এনকোডিং- ম্যাগনেটিক স্ট্রিপ বা মাইক্রোচিপে তথ্যের রেকর্ডিং।

লোকো : লো-কো-ইফিসিয়েন্ট ম্যাগনেটিক স্ট্রিপ (৩০০ অরস্টেড)।

হাইকো : হাই-কো-ইফিসিয়েন্ট ম্যাগনেটিক স্ট্রিপ (নয়েজ-প্রোফ, ৪,০০০ অরস্টেড পর্যন্ত), চৌম্বকীয় স্ট্রিপে সুরক্ষিত তথ্য একটি চৌম্বক ক্ষেত্র ব্যবহার করে এটি মুছে ফেলা কঠিন।

এমবসিং : একটি প্লাস্টিকের কার্ডে অক্ষর এবং অঙ্ক সমন্বিত তথ্য যান্ত্রিকভাবে চাপার একটি পদ্ধতি; যা একটি স্লিপ ছাপিয়ে দ্রুত পেমেন্ট করতে সাহায্য করে।

টিপিং : একটি প্লাস্টিকের কার্ডের ব্যাকগ্রাউন্ড ইমেজ থেকে আলাদা করার জন্য একটি আঁকা ফিল্ম দিয়ে এমবসড চিহ্নগুলোকে ঢেকে রাখা হল টিপিং। প্রায়শই সোনা, রুপা বা অন্যান্য ধাতব রং ব্যবহার করা হয় এবং কালো বা সাদা পেইন্ট যোগ করে প্রয়োজনীয় উজ্জ্বলতা বৃদ্ধি করা হয়।

সিগনেচার স্ট্রিপ : একটি স্বাক্ষর স্থাপন করার জন্য একটি কার্ডের পেছনে অবস্থিত একটি বিশেষ স্ট্রিপ, যা ক্যাপশনসহ বা ছাড়া হতে পারে এবং যা স্বাক্ষরটিকে ঘষা থেকে আটকাতে পারে।

হলোগ্রাম : একটি হলোগ্রাফিক স্টিকার, যা উচ্চ তাপমাত্রার অধীনে একটি কার্ডে চাপা হয়। এটি নকল কার্ড তৈরি থেকে সুরক্ষার একটি অতিরিক্ত স্তর হিসাবে কাজ করে। এটা দুই ধরনের হয় : ২ডি এবং ৩ডি।

## ৫.৬. কার্ড জালিয়াতি (Card Fraud)

একটি কার্ড চুরি করা এবং তাহা পিওএস টার্মিনালে প্রতারণামূলকভাবে ব্যবহার করার জন্য 'পিকপকেট' পদ্ধতিটি ১৯৮০-এর দশকে ব্যবহৃত হয়েছিল। এই ডিজিটাল যুগে তারা তাদের কেলেঙ্কারিতে অত্যাধুনিক সরঞ্জাম স্থাপন করছে। ক্রেডিট কার্ড প্রতারকরা কার্ডের ম্যাগনেটিক স্ট্রিপে এনক্রিপ্ট করা ব্যক্তিগত ডেটা পড়তে এবং নকল করতে 'স্কিমার' মেশিন ব্যবহার করে। এমনকি তাদের আর কার্ড পেতে হয় না, কারণ তারা সরাসরি ক্রেডিট কার্ড লেনদেনের জন্য ব্যবহৃত টেলিকমিউনিকেশন লাইনে ট্যাপ করতে পারে এবং কার্ড ডেটা পেয়ে যেতে পারে। ইতোমধ্যে, অনলাইন লেনদেনের জন্য ক্রেডিট কার্ড ব্যবহার করা প্রচুর বেড়ে গেছে। ফলে কার্ডের ডেটা চুরি করার জন্য নতুন কৌশল হিসাবে 'ফিশিং' আবিষ্কৃত হয়েছে।

প্লাস্টিক কার্ড জালিয়াতি ১৯৮০-এর দশকের শেষের দিকে এবং ১৯৯০-এর দশকের শুরুতে যুক্তরাজ্যে দ্রুততম ক্রমবর্ধমান অপরাধগুলোর মধ্যে একটি। ১৯৯১ সালে কার্ডের জালিয়াতি দ্বিগুণ হয়ে ১৬৫ মিলিয়ন পাউন্ডে পৌঁছে গেছে। প্রধান ব্যাংক এবং পেমেন্ট সোসাইটিগুলো সম্মত হয়েছিল যে জালিয়াতি রোধ করার জন্য সম্মিলিত পদক্ষেপ নেওয়া প্রয়োজন এবং ১৯৯০ সালের সেপ্টেম্বরে তারা প্লাস্টিক জালিয়াতি প্রতিরোধ ফোরাম (পিএফপিএফ) গঠন করে।

১৯৯০-এর দশকের গোড়ার দিকে ফোরাম (ব্যাংক, পেমেন্ট সিস্টেম ইত্যাদি) দ্বারা প্রবর্তিত তাৎক্ষণিক ব্যবস্থাগুলো সেই সমস্ত ক্ষেত্রের ওপর দৃষ্টি নিবদ্ধ করে যেখানে সবচেয়ে বেশি জালিয়াতি সংঘটিত হয়েছিল। যেমন হারানো/চুরি হওয়া কার্ডগুলো দোকানের কাউন্টারে ব্যবহৃত হতো। তাই নিম্নলিখিত উদ্যোগসমূহ গৃহীত হয়—

- লোয়ার ফ্লোর লিমিট প্রবর্তন (যে পরিমাণ লেনদেনের ওপরে একজন খুচরা বিক্রেতাকে কার্ড প্রদানকারীর কাছ থেকে অনুমোদন নিতে হতো) বিশেষ করে জালিয়াতিপ্রবণ খুচরা খাতের জন্য।
- 'হট কার্ড ফাইল'-এর ব্যবহার-হারানো বা চুরি হওয়ার রিপোর্ট করা কার্ডের তালিকা—পয়েন্ট-অফ-সেল (পিওএস) টার্মিনালগুলোতে ইলেকট্রনিকেলি সম্প্রচার করা হয়, যাতে খুচরা বিক্রেতারা স্বয়ংক্রিয়ভাবে একটি কার্ড পরীক্ষা করতে পারে।
- গ্রাহকের কাছে কার্ড বিতরণ করার জন্য আরও নিরাপদ উপায় ব্যবহার করা।
- কার্ডের মধ্যে নিরাপত্তা বৈশিষ্ট্য বৃদ্ধির মধ্যে রয়েছে হলোগ্রাম এবং ম্যাগনেটিক স্ট্রিপে বর্ধিত তথ্য সংরক্ষন করা।
- পিওএস এর মাধ্যমে প্রবর্তিত উদ্যোগের সঙ্গে সহযোগিতা করার জন্য খুচরা বিক্রেতাদের সঙ্গে কাজ করা।
- সব স্তরের পুলিশের সঙ্গে সংলাপ।
- প্রচারণার মাধ্যমে কার্ডধারীদের জন্য ব্যবহারিক পরামর্শ এবং খুচরা বিক্রেতাদের জন্য ভালো অনুশীলন প্রচার করা।

উপরোক্ত উদ্যোগের সাফল্য, প্রতারকদের নতুন ক্ষেত্রগুলোকে টার্গেট করতে সাহায্য করে, যেমন—

### ৫.৬.১. কাউন্টারফিট (Counterfiet)

কাউন্টারফিট হলো দ্রুততম ক্রমবর্ধমান প্রতারণার ধরন। জালিয়াতি করার জন্য ব্যবহৃত কার্ডগুলো সাধারণত হারিয়ে যাওয়া বা চুরি হয়ে যাওয়া কার্ড যা পুনরায় এমবসিং এবং এনকোডিং দ্বারা পরিবর্তন করা হয়েছে, বা যেটি সম্পূর্ণ নতুনভাবে তৈরি করা হয়েছে। একটি কার্ড জাল করার জন্য কার্ডটির তথ্যাদি জানা প্রয়োজন। তারা বিভিন্নভাবে এই সব তথ্য সংগ্রহ করে, তার মধ্যে ইন্টারনেট উল্লেখযোগ্য। তারপর একটি সাদা প্লাস্টিক কার্ড তারা ঐ সমস্ত তথ্য ব্যবহার করে এনকোড করে। পরে সিগনেচার প্যানেল, লোগো, রং ইত্যাদি সংযোগ করে সত্যিকার কার্ডের মতোন একটি কার্ড তৈরি করা হয়।

কখনও কখনও কার্ডের ম্যাগনেটিক স্ট্রিপের তথ্য স্কিমিংয়ের মাধ্যমে পাওয়া যায়। একটি বৈধ কার্ড কয়েক সেকেন্ডের জন্য একটি ম্যাগনেটিক টেপ রিডারের ওপর দিয়ে নেওয়া হয়, ফলে রিডার কার্ডের তথ্য সংগ্রহ করে, যা ব্যবহার করে একটি নকল কার্ড তৈরি করা হয়।

আরেকটি কৌশল হলো 'বাফারিং', যা চৌম্বকীয় স্ট্রিপে সংরক্ষিত তথ্য পরিবর্তন করে থাকে বা কার্ডের সিকিউরিটি কোড ইলেকট্রনিকভাবে অর্জন করতে পারে।

ম্যাগনেটিক স্ট্রিপ কার্ডগুলো জাল করা তুলনামূলকভাবে সহজ কিন্তু স্মার্ট কার্ডগুলো জাল করা অনেক কঠিন। তবে দাবি রয়েছে যে সেগুলো একেবারে টেম্পার-প্রুফ নয়।

এর বিরুদ্ধে সুরক্ষার জন্য আন্তর্জাতিকভাবে সম্মত মানদণ্ডে চিপ কার্ড তৈরি করা হয়েছে। খুচরা বিক্রেতাদেরকেও জাল কার্ড ধরার কৌশলগুলো শেখানো হচ্ছে।

### ৫.৬.২. অ্যাপ্লিকেশন জালিয়াতি (Application Fraud)

কার্ড ইস্যু সম্পর্কিত জালিয়াতি দুটি উপায়ে সংঘটিত হতে পারে—

প্রথমত, তথাকথিত 'ট্রো-নেইম ফ্রড' তখনই ঘটে যখন একজন অপরাধী প্রকৃত ব্যক্তির ব্যক্তিগত বিবরণ সংগ্রহ করতে পারে এবং সেই নামে একটি ক্রেডিট কার্ড তৈরি করতে সক্ষম হয়। অপরাধী তারপর কার্ডটি ব্যবহার করে পণ্য কেনে কিন্তু তার দায় বৈধ কার্ডধারকের কাছে চলে যায়।

দ্বিতীয় ধরনের প্রতারণার মধ্যে রয়েছে মিথ্যা তথ্য দিয়ে কোনো ব্যাংক থেকে একটি কার্ড নেওয়া, সেটি ব্যবহার করে পণ্য ক্রয় করা এবং পরবর্তীতে বিল প্রদান না করে পলাতক থাকা।

### ৫.৬.৩ পিন জালিয়াতি (PIN Fraud)

কার্ড ব্যবহারকারী কার্ড ব্যবহার করার সময় তার পরিচয় প্রমাণ করার প্রক্রিয়া থেকে অন্যান্য জালিয়াতির সূত্রপাত হয়। এটি মূলত ইলেকট্রনিক কার্ড রিডিং মেশিনে যেমন এটিএম বা পসে ডেবিট কার্ডটি ব্যবহারের সময় কার্ডধারী একটি পিন বা পাসওয়ার্ড প্রবেশ করান, যা পরবর্তীতে নেটওয়ার্কের মাধ্যমে প্রেরণের সময় হ্যাকাররা সংগ্রহ করে নিতে পারে। তাই এই পদ্ধতির নিরাপত্তা বাড়ানোর জন্য ব্যবহারকারীর পিনটি এনক্রিপ্ট করে নেটওয়ার্কে পাঠানো হয়। এভাবে নেটওয়ার্কে হ্যাক করে পিন আবিষ্কার করা কঠিন করা হয়ে থাকে।

কার্ডধারকের কাছে পিনটি যেভাবে পাঠানো হয়, কার্ডধারক যেভাবে তা রেকর্ড করে এবং মনে রাখে এবং লেনদেনের সময় টার্মিনালে যেভাবে ব্যবহার করা হয় তা থেকেও উল্লেখযোগ্য নিরাপত্তা ঝুঁকি দেখা দিতে পারে। যদিও কার্ডধারকদের তাদের পিন কার্ডে লিখে রাখা বা কার্ডের সঙ্গে একই জায়গায় রাখা বা কারো কাছে তা বলে দেওয়া সম্পর্কিত বিপদ সম্পর্কে স্পষ্টভাবে সতর্ক করা হয়, কার্ডধারীদের একটি উল্লেখযোগ্য অংশ এই ধরনের পরামর্শ মানতে চায় না, যার ফলে তারা নিজেদেরকে প্রচণ্ড ক্ষতির ঝুঁকিতে রাখে। যার জন্য তারা ব্যক্তিগতভাবে দায়ী থাকবেন।

### ৫.৬.৪. কার্ড নট-প্রেজেন্ট (Cash-not-present)

ইন্টারনেট পেমেন্ট গেটওয়ের মাধ্যমে বিক্রয় লেনদেন বৃদ্ধির ফলে কার্ড নট প্রেজেন্ট জাতীয় জালিয়াতির উল্লেখযোগ্য বৃদ্ধি ঘটেছে। বর্তমানে, ইন্টারনেটে পরিচালিত বেশিরভাগ বাণিজ্যিক লেনদেনে গ্রাহকরা তাদের ক্রেডিট কার্ডের তথ্য ইনপুট দিয়ে পণ্য এবং পরিষেবা ক্রয় করে। এটি অনুমান করা হয়েছে যে ১৯৯৫ সালে ইন্টারনেটে প্রায় ৬৪০ মিলিয়ন ডলার মূল্যের লেনদেন হয়েছিল এবং ২০০৫ সালের শেষ নাগাদ বিশ্বব্যাপী অনলাইন বাণিজ্য ৯৭ বিলিয়ন ডলার থেকে ২৩৮ বিলিয়নের মধ্যে পৌঁছে যায়।

ইন্টারনেট সার্ভিস প্রদানকারীর ডেটাবেস হ্যাক করে অথবা তথ্য আদান-প্রদানের সময় আন-এনক্রিপ্টেড ডেটা আটক করে ক্রেডিট কার্ডের তথ্য অবৈধভাবে সংগ্রহ করা হয়।

এমন অনেক অনলাইন প্রতারক রয়েছে যারা গ্রাহকদের মিথ্যা ক্রেডিট কার্ডের ও মার্চেন্টদের তথ্য ব্যবহার করে। এইসব মার্চেন্ট অনলাইন চুক্তিগুলোকে সম্মান করতে ব্যর্থ হয়।

যুক্তরাজ্যের ব্যাংকিং শিল্প ২০০১ সালে এই ধরনের লেনদেনগুলোকে আরও সুরক্ষিত করতে একটি স্বয়ংক্রিয় ব্যবস্থা প্রয়োগ করে, যার মাধ্যমে মার্চেন্ট কার্ডধারীর বিলিং ঠিকানা এবং কার্ডে বর্ণিত 'কোডেড সংখ্যা' যাচাই করতে পারে।

## ৫.৭. কার্ড জালিয়াতি প্রতিরোধ কৌশল

প্লাস্টিক কার্ড জালিয়াতি প্রতিরোধ করতে চারটি প্রাথমিক কৌশল ব্যবহার করা যেতে পারে।

### ৫.৭.১. কার্ড ইস্যুকারী কর্তৃক করণীয়

প্লাস্টিক কার্ড জালিয়াতির ঝুঁকি কমাতে কার্ড ইস্যুকারীরা বিভিন্ন ধরনের কৌশল অবলম্বন করতে পারে। আর্থিক প্রতিষ্ঠানগুলোর জন্য সবচেয়ে গুরুত্বপূর্ণ বিষয় হলো, এমন কাউকে কার্ড ইস্যু না করা যার পরিচয় সম্বন্ধে তারা নিশ্চিত নয়।

প্লাস্টিক কার্ডগুলো যাতে চুরি না হয় এবং কার্ড এবং পিনগুলো যাতে গ্রাহকদের কাছে নিরাপদে পৌঁছায় তা নিশ্চিত করার জন্য বিভিন্ন পদ্ধতি গ্রহণ করা যেতে পারে। ব্যাংকগুলোও চুরি হওয়া কার্ড এবং পিন সম্পর্কে অবিলম্বে মার্চেন্টদের অবহিত করে সাহায্য করতে পারে। কার্ডের ওপর কার্ডধারীর ছবিও ছাপানো যেতে পারে।

EFTPOS-এ জালিয়াতি প্রতিরোধ করার জন্য ব্যবহৃত প্রধান কৌশলগুলোর মধ্যে একটি হলো লোয়ার ফ্লোর লিমিট নির্ধারণ করা। লোয়ার ফ্লোর লিমিট হলো এমন একটি লিমিট যার বেশি পরিমাণ লেনদেন হলে ব্যাংকের অনুমোদনের প্রয়োজন হয়।

পরিশেষে, স্মার্ট কার্ডের জালিয়াতি কমানোর উদ্দেশ্যে বিভিন্ন লেনদেন পর্যবেক্ষণ কৌশল অবলম্বন করা হয়েছে—যাতে দ্রুত প্রতারণামূলক লেনদেনগুলো চিহ্নিত করা যায় এবং লেনদেনের সর্বোচ্চ লিমিট সীমিত করা যায়।

### ৫.৭.২. মার্চেন্ট কর্তৃক করণীয়

মার্চেন্টের সঙ্গে জড়িত প্রতারণা আর্থিক প্রতিষ্ঠানের জন্য একটি বড় সমস্যা, কারণ মার্চেন্ট বা তাদের কর্মচারীদের গ্রাহকের কার্ড পরিচালনা করা কম্পিউটার নেটওয়ার্কগুলোতে অ্যাক্সেস করা এবং লেনদেনের তথ্য পরিবর্তন করার সুযোগ দেওয়া হয়।

পরিশেষে, মার্চেন্টকে গ্রাহকদের সন্দেহজনক আচরণ এবং চেহারা পরীক্ষা করা উচিত। যে গ্রাহকগণ দ্রুত পণ্য নির্বাচন, যারা নির্বাচিত পণ্যের প্রকৃতির সঙ্গে অসঙ্গতিপূর্ণ পোশাক পরে, যে গ্রাহকরা ইস্যুয়িং ব্যাংকের কাছে অনুমোদনের কলগুলো আটকানোর প্রয়াসে বিভিন্ন ভাগে ভাগ করে কেনাকাটা করে, যারা ফ্লোর লিমিটের মধ্যে অনেকবার ক্রয় করে এবং যারা একই আইটেম অনেকগুলো ক্রয় করে কিন্তু বিভিন্ন রং ও সাইজের, তাদেরকে মার্চেন্ট সন্দেহজনক মনে করতে পারেন। দুর্ভাগ্যবশত, সত্যিকারের গ্রাহকদের নিরুৎসাহিত করার ভয়ে মার্চেন্টগণ এই সমস্ত কৌশল ব্যবহার করা থেকে বিরত থাকেন।

### ৫.৭.৩. কার্ডধারী কর্তৃক করণীয়

একজনের কার্ড, পিন বা পাসওয়ার্ড এর সুরক্ষা প্রদান করা হলো প্রাথমিক অপরাধ প্রতিরোধের কৌশল, যা কার্ডধারীদের গ্রহণ করতে হবে। যদিও কার্ডধারীদের তাদের পিন প্রকাশ না করার, পিনটি কার্ডের সঙ্গে না রাখার বা কার্ডে এটি না লেখার পরামর্শ দেওয়া হয়, গবেষণায় দেখা গেছে যে ২০ থেকে ৭০ শতাংশ লোক এই ধরনের পরামর্শ মানে না।

### ৫.৭.৪. প্রযুক্তিগত সমাধান (Technical Solution)

প্লাস্টিক কার্ড ও পেমেন্ট সিস্টেমের সঙ্গে সম্পর্কিত নিরাপত্তা ঝুঁকি কমাতে প্রযুক্তিগত সমাধানের একটি বিস্তৃত পরিসর তৈরি করা হয়েছে।

#### ৫.৭.৪.১. কার্ড কাউন্টার ফিশিংয়ের বিরুদ্ধে সুরক্ষা

প্লাস্টিক কার্ডের নিরাপত্তা বাড়ানোর জন্য এবং তাদের পরিবর্তন বা নকল করা আরও কঠিন করার জন্য বিভিন্ন কৌশল তৈরি করা হয়েছে। এর মধ্যে রয়েছে মাইক্রো চিপস, হলোগ্রাম, এমবসড ক্যারেক্টার, ট্যাম্পার-এভিডেন্ট সিগনেচার প্যানেল, উন্নত কার্ড ভ্যালিডেশন প্রযুক্তিসহ ম্যাগনেটিক স্ট্রাইপ এবং ইন্ডেন্ট প্রিন্টিংয়ের ব্যবহার।

#### ৫.৭.৪.২. কার্ড সীমাবদ্ধতা (Card Restriction)

প্লাস্টিক কার্ড ব্যবহারের মাধ্যমে বড় আকারের জালিয়াতির ঝুঁকি এড়ানো উদ্দেশ্যে কার্ডভিত্তিক লেনদেনের ওপর লিমিট প্রদান বা প্লাস্টিক কার্ডে সঞ্চিত অর্থের পরিমাণের ওপর লিমিট স্থাপন করা যেতে পারে। কার্ডের ভেলিডিটির (validity) একটি সীমা থাকতে পারে।

#### ৫.৭.৪.৩. জালিয়াতি শনাক্তকরণ সফটওয়্যার

এমন সফ্টওয়্যারও তৈরি করা হয়েছে, যা প্লাস্টিক কার্ডধারীদের ব্যয়ের ধরন বিশ্লেষণ করতে সক্ষম এবং অননুমোদিত লেনদেন সম্পর্কে সতর্ক করে। মার্চেন্ট ডিপোজিট পর্যবেক্ষণ কৌশলগুলো দুর্নীতিগ্রস্ত মার্চেন্টের অযৌক্তিক দাবি নির্ণয় করতে পারে। PRISM (প্রোঅ্যাকটিভ ফ্রড রিস্ক ম্যানেজমেন্ট) নামে একটি সফ্টওয়্যার প্যাকেজ রয়েছে, যা হারিয়ে যাওয়া কার্ড, চুরি হওয়া কার্ড, জাল কার্ড, জালিয়াতি অ্যাপ্লিকেশন, না পাওয়া কার্ড, মেল অর্ডার, ফোন অর্ডার, ক্যাটালগ বিক্রয় এবং মার্চেন্ট প্রতারণা নির্ণয় করতে পারে। সিস্টেমের প্রয়োজনীয়তা এবং কনফিগারেশনের ওপর নির্ভর করে এটির দাম ডলার ৩৮৪,০০০ থেকে ১.৯২ মিলিয়নের মধ্যে হতে পারে। যদিও প্রাথমিক ইনস্টলেশন খরচ অনেক বেশি, জালিয়াতি প্রতিরোধ এবং শনাক্তকরণের মাধ্যমে প্রাপ্ত সুবিধাগুলো বড় প্রতিষ্ঠানের জন্য এটিকে লাভজনক করে তোলে।

#### ৫.৭.৪.৪. উন্নত ক্রিপ্টোগ্রাফি (Improred cryptography)

ক্রিপ্টোগ্রাফি হলো ইলেকট্রনিক ব্যাংকিং নিরাপত্তা ব্যবস্থার প্রধান ভিত্তি। নেটওয়ার্কের ভিতর দিয়ে ডেটা ট্রান্সমিশন করার সময় ক্রিপ্টোগ্রাফি ব্যবহার করা হয়। এটি মাস্টারকার্ড এবং ভিসা ইন্টারন্যাশনালের একটি যৌথ উদ্যোগ যাকে সিকিউর ইলেকট্রনিক লেনদেন প্রোটোকল বলা হয়। ইলেকট্রনিক ক্যাশ সিস্টেমগুলোকে সুরক্ষিত করার জন্যও এটি ব্যবহার করা হয়। এই পদ্ধতিতে

ডেটাকে আপস করা থেকে রক্ষা করতে পাবলিক কী এনক্রিপশন ব্যবহার করা হয়।

### ৫.৭.৪.৫. ইএমভি (EMV)

**ক. ইএমভি কী?**

ইএমভি হলো স্মার্ট কার্ড যা ডেবিট বা ক্রেডিট হতে পারে। ইএমভি যৌথভাবে ইউপে, মাস্টারকার্ড এবং ভিসা দ্বারা তৈরি করা হয়েছে। সম্প্রতি জেসিবি এবং অ্যামেক্সও ইএমভিতে যোগ দিয়েছে।

একটি স্মার্ট কার্ড হলো একটি কম্পিউটার চিপভিত্তিক কার্ড, যাতে নিম্নলিখিতগুলো থাকে—

- মেমোরি
- স্টোরেজ স্পেস যা কার্ড আইডি, কার্ডধারীর আইডি, পিন, অনুমোদনের স্তর, নগদ ব্যালেন্স, ক্রেডিট লিমিট সংরক্ষণ করে।
- একটি অপারেটিং সিস্টেম যেমন—নেটিভ ওএস, মাল্টোস, বা জাভাকার্ড
- অ্যাপ্লিকেশন প্রোগ্রামের রুটিনসমূহ

ইএমভি ইএমভিকো দ্বারা সংজ্ঞায়িত বাধ্যতামূলক এবং ঐচ্ছিক অপশনগুলো অন্তর্ভুক্ত করেছে যেমন—

- স্ট্যাটিক ডেটা অথেন্টিকেশন (এসডিএ) এর মাধ্যমে সুরক্ষিত কার্ড অথেন্টিকেশন পদ্ধতি (সিএএম)।
- ডাইনামিক ডেটা অথেনটিকেশন (ডিডিএ)।
- সম্মিলিত ডেটা অথেনটিকেশন (সিডিএ)।
- সুরক্ষিত কার্ডধারী যাচাইকরণ পদ্ধতি (সিভিএম)।
- বর্ধিত ঝুঁকি ব্যবস্থাপনা।
- অ্যাপ্লিকেশন প্রোগ্রামিং ইন্টারফেস (API)।

**খ. ইএমভিকো (EMVCO) কী?**

ইএমভিকো হলো একটি কোম্পানি যা ইউরোপে ইন্টারন্যাশনাল, মাস্টারকার্ড ইন্টারন্যাশনাল এবং ভিসাস ইন্টারন্যাশনাল দ্বারা ১৯৯৯ সালের ফেব্রুয়ারিতে গঠিত হয়। ২০০২ সালে, মাস্টারকার্ড ইন্টারন্যাশনাল দ্বারা ইউরোপে ইন্টারন্যাশনালের অধিগ্রহণ করা হয়। ২০০৪ এবং ২০০৯ সালে, জেসিবি এবং এমেক্স যথাক্রমে ইএমভিকোতে যোগদান করে। বর্তমানে, এমেক্স, জেসিবি, মাস্টারকার্ড এবং ভিসার প্রত্যেকের ২৫% শেয়ার রয়েছে।

**গ. ইএমভি-এর সুবিধা**

- কার্ড জালিয়াতি প্রতিরোধ করুন।
- অফলাইনে নিরাপদ লেনদেন, ফলে সমস্ত লেনদেন অনলাইনে করার দরকার নেই। অনলাইন খরচ বাঁচায়।
- চিপ লায়াবিলিটি সিফ্টিং।
- কন্টাক্টলেস মাস্টারকার্ড পেপাসের মতো বিভিন্ন প্রোগ্রাম বাস্তবায়ন করা সহজ।
- একটি নন-ইএমভি ইস্যুয়ার বা অ্যাকোয়ারারে থেকে বেশি আয়।

**ঘ. কেন ব্যাংকগুলোকে ইএমভিতে যেতে হবে?**

- ইন্টারঅপারেবিলিটি।
- অন্য ইস্যুয়ারের কার্ড গ্রহণ, নিরাপত্তা এবং পেমেন্ট ফাংশন।
- লায়াবিলিটি সিফ্ট।

উন্নত নিরাপত্তা

- ক্রিপ্টোগ্রাফি, কার্ড এবং টার্মিনালের মধ্যে অফলাইন ঝুঁকি ব্যবস্থাপনা
- হারিয়ে যাওয়া বা চুরি হওয়া কার্ড ব্যবহার করে সম্ভাব্য জাল-জালিয়াতির বিরুদ্ধে সুরক্ষা (অফলাইন পিনের মাধ্যমে)।

উন্নত নিয়ন্ত্রণ

- অফ-লাইন/জোরপূর্বক অন-লাইনের ক্ষেত্রে অত্যাধুনিক অনুমোদন সংক্রান্ত সিদ্ধান্ত গ্রহণ।
- ইস্যুয়ারের ঝুঁকি নিয়ন্ত্রণ করে।
- চিপের অভ্যন্তরে রক্ষিত অ্যাপ্লিকেশন ব্যবহার করে টার্মিনালে গ্রাহক-কেন্দ্রিক সিদ্ধান্ত গ্রহণ।

অপারেশনাল সুবিধা

- বেশি বেশি অফ-লাইন প্রক্রিয়াকরণ, ফলে কম চার্জব্যাক ও কার্ডের দীর্ঘায়ু বৃদ্ধি পায়।
- ইস্যুয়িং ব্যাংক টার্মিনাল ব্যবহার করে কার্ড আপডেট করতে পারে।

- 'স্ক্রিপ্টিং'এর মাধ্যমে প্যারামিটার পরিবর্তন করা।
- নতুন অ্যাপ্লিকেশন যোগ করা ও তা সক্রিয় করা—যেমন কার্ডভিত্তিক লায়াবিলিটি।

**ঙ. মেগ-স্ট্রিপ কার্ডে জালিয়াতির ঝুঁকি**

i কার্ডটি ৫০ ডলারের একটি ছোট ডিভাইস দিয়ে কপি করা যেতে পারে।

ii ট্র্যাকে তথ্য এনক্রিপ্ট করা হয় না ফলে চুরি করা ডেটা দিয়ে খুব সহজে কার্ড পার্সোনালাইজেশান করা সম্ভব।

iii একটি জাল কার্ড পার্সোনালাইজেশন করার আগে কপি করা ডেটা খুব সহজেই পরিবর্তন করা যেতে পারে।

**চ. ইএমভি কীভাবে জাল জালিয়াতি রক্ষা করে?**

i চিপ ডেটা অনুলিপি করা সহজ নয় (বিলিয়ন ডলার বিনিয়োগের মাধ্যমে সম্ভব হতে পারে)।

ii একটি ডিডিএ কার্ডে, চিপ ডেটা অনুলিপি করা এবং জাল কার্ড তৈরি করা সম্ভব নয়, কারণ এই ধরনের কার্ডের ভেতরে প্রসেসর দ্বারা একটি ডায়নামিক কী তৈরি করে যা প্রতিটি ডিডিএ কার্ডের জন্য অনন্য, যাকে আমরা আইসিসি কী বলি। কার্ড ডেটা একটি আইসিসি প্রাইভেট কী দ্বারা স্বাক্ষরিত যা সংশ্লিষ্ট আইসিসি পাবলিক কী ছাড়া ডিক্রিপ্ট করা যাবে না।

দ্রষ্টব্য : ডিডিএ এর অর্থ হলো ডায়নামিক ডেটা অথেন্টিকেশন যা—

১. আইসিসি এবং 'টার্মিনাল ডাইনামিক অ্যাপ্লিকেশন ডেটার' সত্যতা এবং অখণ্ডতা প্রদান করে (আইসিসি প্রাইভেট কী দ্বারা স্বাক্ষরিত)।

২. কার্ডটি পার্সোনালাইজেশনের পরে আইসিসিতে রক্ষিত ডেটার কোনো পরিবর্তন হলে তা শনাক্তকরণে সাহায্য করে।

৩. রিপ্লে আক্রমণ এবং আইসিসি নকল প্রতিরোধ করে।

iii 'একটি ডিডিএ কার্ডে কার্ডের তথ্য তিনবার এনক্রিপ্ট করা হয় ক) কার্ড কী (আইসিসি কীও বলা হয়, এটি কার্ড নির্দিষ্ট কী) দ্বারা, খ) ইস্যুয়ারের ব্যক্তিগত কী (ইস্যুয়ার হোস্ট দ্বারা তৈরি করা আরএসএ কী) দ্বারা ও, গ) CA স্বাক্ষরিত IPK (ইএমভিকো সিএ এর প্রাইভেট কী দ্বারা এনক্রিপ্ট করা ইস্যুয়ার পাবলিক কী)।

iv পাবলিক কী প্রাইভেট কী ডিক্রিপ্ট করতে পারে এবং সমস্ত টার্মিনালের EMVCO তে CA পাবলিক কী থাকে।

v পার্সোনালাইজেশনের সময় ইস্যুকারীর দ্বারা চিপ কার্ডে সেট করা IAC (ইস্যুয়ার অ্যাকশন কোড) অনুসারে একটি নির্দিষ্ট লেনদেনের জন্য (লেনদেনের পরিমাণ, ফ্রিকোয়েন্সি ও প্রকারের ওপর নির্ভর করে) কী পদক্ষেপ নেওয়া হবে তা কার্ড নিজেই সিদ্ধান্ত নিতে পারে। যেমন অফলাইনে অনুমোদন প্রদান, অফলাইনে প্রত্যাখ্যান করা বা অনলাইনে চলে যাওয়া ইত্যাদি।

vi অনলাইন লেনদেনের ক্ষেত্রে ডিক্রিপশন প্রক্রিয়ায় কার্ডের ডেটা পাওয়ার পরে, কার্ড ডেটা পুনরায় ইউডিকে (ইউনিক ডেরিভেটিভ, কী যাহা একটি TDES কী) দ্বারা এনক্রিপ্ট করা হয় এবং ARQC (অথোরাইজেশন রিকোয়েস্ট কী) তৈরি করা হয়। এই UDK পার্সোনালাইজেশনের সময় এমডিকে (মাস্টার ডেরিভেটিভ কী) থেকে তৈরি করা হয়। এই MDK-কে শেয়ার করা হয় এবং ইস্যুকারী হোস্টে সংরক্ষণ করা হয়। যখন একটি লেনদেনের ARQC ইস্যুকারীর হোস্টে অনলাইনে আসে, তখন UDK দিয়ে ডেটা ডিক্রিপ্ট করে (যেহেতু হোস্টে এমডিকে আছে)। যদি কার্ডের ডেটা সঠিক পাওয়া যায় এবং ইস্যুকারী হোস্টে অন্যান্য বৈধতা পাওয়া যায়, তখন ইস্যুকারী হোস্ট ইউডিকে দ্বারা স্বাক্ষরিত একটি ARPC (অথোরাইজেশন রেস্পন্স কোড) ফেরত পাঠায়। যেহেতু কার্ডটিতে UDK রয়েছে (আগে উল্লেখ করা হয়েছে, পার্সোনালাইজেশনের সময় কার্ডটিতে UDK ঢোকানো হয়েছে), এটি ARPC-কে ডিক্রিপ্ট করতে পারে এবং ইস্যুকারী হোস্ট কী পরামর্শ দিয়েছেন তা দেখতে পারে।

**ছ একটি মেগ-স্ট্রিপ কার্ড এবং চিপ কার্ডের মূল বিষয়বস্তু কী কী?**

মেগ-স্ট্রিপ কার্ডে ট্রাক১ এবং ট্রাক২ ডেটা রয়েছে যা কার্ডের নাম, কার্ড নম্বর, মেয়াদ শেষ হওয়ার তারিখ, সিভিভি, সিভিসি ইত্যাদি স্টোর করে।

অন্যদিকে চিপ কার্ডে রয়েছে—

i মেগ-স্ট্রিপ ডেটার সমস্ত তথ্য

ii আইসিসি পাবলিক কী-এর অধীনে কার্ড ডেটা

iii ইস্যুকারী প্রাইভেট কী-এর অধীনে ICC পাবলিক কী

iv ইস্যুকারী পাবলিক কী যাহা CA এর প্রাইভেট কী

v UDK (অনলাইনে লেনদেনের ক্ষেত্রে ARQC তৈরি করার জন্য)

vi UDK (মেক), UDK (Enc) (ইস্যুকারীর স্ক্রিপ্ট আপডেটের জন্য)একই UDK-এর মানগুলো কার্ড এবং ইস্যুকারীর হোস্টে রাখা হয়। এইভাবে এটি ইস্যুকারীর দ্বারা প্রেরিত বা গৃহীত স্ক্রিপ্টগুলোকে যাচাই ও আপডেট করা হয়।

**৬. ইন্টারনেট ব্যাংকিং**

ইন্টারনেট ব্যাংকিং আই-ব্যাংকিং বা অনলাইন ব্যাংকিং নামেও পরিচিত। ইন্টারনেট ব্যাংকিং হলো এমন একটি ব্যবস্থা, যা গ্রাহকরা ইন্টারনেটের মাধ্যমে তাদের বাড়ি, অফিস বা বিশ্বের যে কোনো জায়গা থেকে তাদের অ্যাকাউন্টে অ্যাক্সেস করতে পারেন। এই পরিষেবাটি পেতে, গ্রাহককে তার ব্যাংক থেকে একটি আইডি এবং পাসওয়ার্ড নিতে হয় এবং তার ইন্টারনেট সংযোগসহ একটি কম্পিউটার থাকতে হয়।

**৬.১. ইন্টারনেট ব্যাংকিং পাসওয়ার্ড**

গ্রাহক যখন প্রথমবার আই-ব্যাংকিং অ্যাক্সেস করেন, তখন সিস্টেম তার পাসওয়ার্ড পরিবর্তন করতে বলে। গ্রাহককে ব্যাংকের পাসওয়ার্ড নীতি অনুযায়ী পাসওয়ার্ড পরিবর্তন করতে হবে। উদাহরণস্বরূপ, একটি ব্যাংক নিম্নলিখিত পাসওয়ার্ড নীতি থাকতে পারে—

- পাসওয়ার্ডের দৈর্ঘ্য সর্বনিম্ন ৬ অক্ষর এবং সর্বোচ্চ ১২ অক্ষর হতে হবে।
- ব্যবহারকারী আইডি পাসওয়ার্ডের একটি অংশ হিসাবে ব্যবহার করা যাবে না।
- পাসওয়ার্ডে কমপক্ষে ১টি বড় হাতের, কমপক্ষে ১টি ছোট হাতের, ১টি সংখ্যা এবং একটি প্রতীকী অক্ষর থাকতে হবে।
- একই সংখ্যা বা অক্ষর পর পর ২ বার ব্যবহার করা যাবে না।

নিম্নলিখিতগুলো বৈধ পাসওয়ার্ড :
Joyful7, raiN573

নিম্নলিখিতগুলো বৈধ পাসওয়ার্ড নয় :
Joy7, rain573, Rain666, aaAmin2

**৬.২. ইন্টারনেট ব্যাংকিং ফাংশন :**

গ্রাহকরা নগদ লেনদেন ছাড়া প্রায় সব ধরনের ব্যাংকিং কার্যক্রম আই-ব্যাংকিংয়ের মাধ্যমে করতে পারেন।

**অ্যাকাউন্ট সামারি**

গ্রাহক কারেন্ট, সেভিংস, টার্ম ডিপোজিট এবং রিটেল লোন অ্যাকাউন্টের তালিকা এবং অ্যাকাউন্টের মুদ্রায় প্রতিটি অ্যাকাউন্টে বর্তমান ব্যালেন্স দেখতে সক্ষম হবেন। গ্রাহকের পছন্দের মুদ্রায় ও গ্রাহকের অ্যাকাউন্টের ব্যালেন্সের মূল্যমান দেখানো যেতে পারে।

**অ্যাকাউন্টের বর্ণনা**

গ্রাহক একটি নির্দিষ্ট অ্যাকাউন্ট (সেভিংস, চেকিং অ্যাকাউন্ট, মেয়াদি আমানত, বা ঋণ অ্যাকাউন্ট) বেছে নিতে পারেন এবং অ্যাকাউন্টের বিশদ বিবরণ দেখতে পারেন যেমন খোলার তারিখ, মেয়াদপূর্তির তারিখ, বকেয়া ব্যালেন্স, অর্জিত সুদ, প্রদত্ত সুদ, লিমিটের পরিমাণ ইত্যাদি।

**অ্যাকাউন্ট কার্যকলাপ**

গ্রাহক প্রদত্ত দুটি তারিখের মধ্যবর্তী দিনগুলোর জন্য একটি প্রদত্ত অ্যাকাউন্টে লেনদেনের কার্যকলাপ দেখতে পারেন।

**তহবিল স্থানান্তর**

গ্রাহক তার এক অ্যাকাউন্ট থেকে ব্যাংকের অন্য অ্যাকাউন্টে বা অন্য ব্যাংকের অ্যাকাউন্টে তহবিল স্থানান্তর করতে পারেন।

**মেয়াদী আমানত (টিডি) খোলা**

গ্রাহক ব্যাংকে তার কারেন্ট বা সঞ্চয়ী অ্যাকাউন্ট থেকে তহবিল স্থানান্তর করে একটি মেয়াদী আমানত খুলতে পারেন।

**মেয়াদি আমানত পরিবর্তন করা**

গ্রাহক বিদ্যমান টার্ম ডিপোজিট অ্যাকাউন্টের মেয়াদ ও সুদ সংক্রান্ত নির্দেশের পরিবর্তন করতে পারেন।

**মেয়াদি আমানত বন্ধ করা**

গ্রাহক তার মেয়াদি আমানতের আংশিক বা সম্পূর্ণ সেটির মেয়াদ শেষ হওয়ার আগেই বন্ধ করতে পারেন। তাকে নিয়ম অনুযায়ী প্রযোজ্য Penalty দেখানো হবে।

**ঋণ পরিশোধ**

গ্রাহক ঋণের কিস্তি পূর্ণ বা আংশিক পরিশোধ করতে পারেন। টাকা তার ডিপোজিট অ্যাকাউন্ট থেকে স্থানান্তর করা হবে।

**প্রাথমিক এবং চূড়ান্ত নিষ্পত্তি**

গ্রাহক ঋণের পুরোটাই মেয়াদপূর্তির পূর্বেই পরিশোধ করতে পারেন। টাকা তার ডিপোজিট অ্যাকাউন্ট থেকে স্থানান্তর করা হবে।

**স্ট্যান্ডিং ইন্‌স্ট্রাকশ**

গ্রাহক তার ডিপোজিট অ্যাকাউন্ট থেকে অন্য ডিপোজিট অ্যাকাউন্টে (নিজ বা তৃতীয় পক্ষ) প্রতি সপ্তাহ/মাস/ত্রৈমাসিক/বছরে একটি নির্দিষ্ট তারিখে একটি নির্দিষ্ট পরিমাণ তহবিল স্থানান্তর করতে স্ট্যান্ডিং ইন্‌স্ট্রাকশন গঠন বা সেট আপ করতে পারেন। তিনি স্থায়ী নির্দেশ বাস্তবায়নের শুরুর তারিখ এবং শেষ হওয়ার তারিখ উল্লেখ করতে পারেন।

অ্যাকাউন্টধারীগণ প্রতিটি অ্যাকাউন্টের জন্য এক বা একাধিক এস. আই. সেট-আপ করতে পারেন এবং তাদের অগ্রাধিকার (Priority) নির্ধারণ করতে পারে। নির্দেশাবলি এককালীন স্থানান্তরের জন্য বা পূর্ব-নির্ধারিত ফ্রিকোয়েন্সিতে বার বার স্থানান্তরের জন্য সেটআপ করা যেতে পারে।

**প্রাপক মেইনটেন্যান্স**

গ্রাহক 'থার্ড-পার্টি ফান্ড ট্রান্সফারের জন্য তৃতীয় পক্ষের অ্যাকাউন্ট নম্বর এবং অন্যান্য বিবরণ উল্লেখ করে একটি টেমপ্লেট সেট আপ করতে পারেন। 'তৃতীয় পক্ষ মানে অন্য একজন ব্যক্তি যার একই ব্যাংকে অ্যাকাউন্ট আছে। তবে, একটি শিক্ষা প্রতিষ্ঠান বা ইউটিলিটি কোম্পানি একটি 'তৃতীয় পক্ষ নয়। 'তৃতীয় পক্ষ স্থানান্তরের সময়' তালিকায় কার্যকরী এবং লভ্য হতে, এই ধরনের এন্ট্রিগুলোকে একজন ব্যাংক অফিসার দ্বারা অনুমোদিত করতে হবে।

**তৃতীয় পক্ষ স্থানান্তর**

গ্রাহক তার একটি অ্যাকাউন্ট থেকে ব্যাংকের মধ্যে অন্য তৃতীয় আরেকটি অ্যাকাউন্টে তহবিল স্থানান্তর করতে পারেন। 'থার্ড পার্টি' অ্যাকাউন্টটি অবশ্যই 'প্রাপক মেইনটেন্যান্স' ব্যবহার করে সিস্টেমে পূর্বেই রেকর্ড করতে হবে এবং তালিকায় এটি সহজলভ্য করার জন্য একজন ব্যাংক অফিসারের দ্বারা অনুমোদিত হতে হবে।

**বিবৃতি অনুরোধ**

গ্রাহক একটি প্রয়োজনীয় সময়ের জন্য একটি অ্যাকাউন্টের স্টেটমেন্টের জন্য একটি অনুরোধ করতে পারেন। ব্যাংক এই অনুরোধটি পাওয়ার পর ম্যানুয়ালি তা কার্যকর করবে।

**চেক বুক অনুরোধ**

গ্রাহক ব্যাংকের অফার করা সেট থেকে পছন্দসই পাতার সংখ্যা বেছে নিয়ে অ্যাকাউন্টের বিপরীতে একটি চেক বইয়ের জন্য অনুরোধ করতে পারেন।

**চেক বন্ধ করার জন্য অনুরোধ**

গ্রাহক একটি অ্যাকাউন্ট এর বিপরীতে ইস্যুকৃত চেকের এক বা একাধিক পাতা উল্লেখ করে ঐ সমস্ত পাতার অনুকূলে টাকা প্রদান বন্ধ করতে পারেন। এনক্যাশমেন্ট বন্ধের কারণও তিনি উল্লেখ করতে পারেন।

**চেক স্ট্যাটাস জানা**

গ্রাহক একটি অ্যাকাউন্ট নম্বর এবং সেই অ্যাকাউন্টের অনুকূলে ইস্যুকৃত চেক নম্বর লিখে সেই চেকের স্ট্যাটাস জানতে পারেন। চেক ফেরত এলে, বা বন্ধ করা হলে, প্রত্যাখ্যানের কারণও দেখানো হবে।

**এফএক্স রেট অনুসন্ধান**

গ্রাহক এই ফাংশনটি ব্যবহার করে ব্যাংক যে FX হারগুলো অফার করে তা জানতে পারেন। প্রদর্শিত হার হলো টিটি, ক্যাশ এবং ডিডি রেট।

**সুদের হার অনুসন্ধান**

গ্রাহক ব্যাংকের দেওয়া সঞ্চয়ী এবং মেয়াদি আমানতের সুদের হার সম্পর্কে জানতে পারেন।

**পাসওয়ার্ড পরিবর্তন করা**

গ্রাহক এই ফাংশন ব্যবহার করে স্বেচ্ছায় ইন্টারনেট পাসওয়ার্ড পরিবর্তন করতে পারেন। উপরন্তু, ব্যবহারকারীকে প্রথমবার সিস্টেমে ঢোকার সময় এবং নির্ধারিত কিছুদিন পর পর (যেমন ৯০ দিন পর পর) সিস্টেম দ্বারা পাসওয়ার্ড পরিবর্তন করতে বাধ্য করা হয়। উভয় ক্ষেত্রেই, পাসওয়ার্ডটি ব্যাংকের দ্বারা সংজ্ঞায়িত নীতির সঙ্গে সঙ্গতিপূর্ণ হওয়া প্রয়োজন।

**লেটার অব ক্রেডিট ইস্যু করা**

গ্রাহক (কোম্পানি) ইন্টারনেট ব্যাংকিং ব্যবহার করে লেটার অব ক্রেডিট তৈরি করতে পারেন। কোম্পানির একজন কর্মকর্তা তার অফিস থেকে এলসি সংক্রান্ত ফর্ম অনলাইনে পূরণ করবেন। অন্য একজন উচ্চ-স্তরের কর্মকর্তা এলসি অনুমোদন করবেন এবং ব্যাংকে পাঠাবেন। সংশ্লিষ্ট ব্যাংক কর্মকর্তা এন্ট্রিগুলো পরীক্ষা করবেন এবং তা সংযুক্ত স্কেন (scan) কপির সঙ্গে যাচাই করবেন এবং অনুমোদন করবেন। ব্যাংকের অনুমোদনের পরে, প্রয়োজনীয় অ্যাকাউন্টিং এন্ট্রিগুলো কোর ব্যাংকিং সিস্টেমে রেকর্ড হয়ে যাবে এবং একটি সুইফট বার্তা চলে যাবে।

এলসি স্ক্রিনে (কোম্পানির একজন কর্মকর্তার দ্বারা) ডেটা এন্ট্রিতে একাধিক স্ক্রিন থাকবে, যাতে Save এবং Submit অপশন থাকবে। Save অপশনটি প্রতিটি স্ক্রিনে টাইপ করা আংশিক বা অসম্পূর্ণ ডেটা সংরক্ষণের সুবিধা দেবে। Submit অপশনটি দেখা দিলে তা ক্লিক করে ডেটা ব্যাংকে জমা দেওয়া হবে। সিস্টেম সমস্ত স্ক্রিনে টাইপ করা ডেটার যাচাই করবে এবং কোনো ত্রুটি পাওয়া গেলে তা ব্যবহারকারীর কাছে প্রদর্শিত করা হয়।

যাচাইকরণ ও নিশ্চিতকরণ (কোম্পানির একজন উচ্চস্তরের কর্মকর্তা দ্বারা) স্ক্রিনটি এল.সি. submit করার পর প্রদর্শিত হবে এবং এটি একটি একক স্ক্রিন হবে। প্রতিটি স্ক্রিনের নিচে অডিট তথ্য প্রদর্শিত হবে, যার বিষয়বস্তু হবে এল.সি. প্রস্তুতকারীর নাম, তারিখ এবং অনুমোদনকারীর নাম এবং এর সঙ্গে সম্পর্কিত তারিখ।

**পরিবর্তন করা**

গ্রাহক কিছু নির্দিষ্ট পরিস্থিতিতে এলসি পরিবর্তন করতে পারেন। সেক্ষেত্রে একই ব্যবহারকারীর দ্বারা এলসি এর পরিবর্তন শুরু করতে হবে। উপরন্তু, পরিবর্তন করা লেনদেনটি হয় একটি অসম্পূর্ণ অবস্থায় থাকতে হবে অথবা অনুমোদনকারী কর্তৃক প্রত্যাখ্যাত হতে হবে। প্রতিটি স্ক্রিনের নিচে অডিট তথ্য প্রদর্শিত হবে যার বিষয়বস্তু হবে সূচনাকারীর নাম এবং তারিখ এবং অনুমোদনকারীর নাম এবং এর সঙ্গে সম্পর্কিত তারিখ।

**অনুমোদন**

অনুমোদনকারী শুধু সেইসব এলসি লেনদেন অনুমোদন করতে পারেন যার জন্য তার অধিকার রয়েছে। অধিকার, সূচনাকারী এবং লেনদেনের অনুমোদিত সীমার ওপর ভিত্তি করে হবে। একবার লেনদেন অনুমোদিত হলে তা সরাসরি কোর ব্যাংকিং সিস্টেমে পাঠানো হয়।

অনুমোদনকারী একটি এলসি প্রত্যাখ্যান করতে পারেন। প্রত্যাখ্যানের কারণ উল্লেখ করার একটি সুবিধা প্রদান করা হয়েছে। প্রতিটি স্ক্রিনের নিচে অডিট তথ্য প্রদর্শিত হবে, যার বিষয়বস্তু হবে সূচনাকারীর নাম এবং তারিখ এবং অনুমোদনকারীর নাম এবং এর সঙ্গে সম্পর্কিত তারিখ।

**৬.৩. ইন্টারনেট ব্যাংকিংয়ে জালিয়াতি**

আমরা যদি ওপরে উল্লিখিত ইন্টারনেট ব্যাংকিং সিস্টেমের আওতায় থাকা কার্যকারিতাগুলো দেখি, তাহলে আমরা দেখতে পাব যে একজন প্রতারক যদি একজন গ্রাহকের আইডি এবং পাসওয়ার্ড জানতে পারে, তাহলে সে সহজেই সিস্টেমে অ্যাক্সেস পেতে পারে এবং নিম্নলিখিতগুলো করতে পারে :

১. ঐ গ্রাহকের সব অ্যাকাউন্টের নম্বর, অ্যাকাউন্ট ব্যালেন্স এবং লেনদেনের ইতিহাস পেতে পারেন (গোপনীয় তথ্য চুরি)।
২. গ্রাহকের একটি অ্যাকাউন্ট থেকে গ্রাহকের অন্য অ্যাকাউন্টে বা একটি ইউটিলিটি কোম্পানির অ্যাকাউন্টে অর্থ স্থানান্তর করতে পারে (হয়রানি)।
৩. গ্রাহকের অ্যাকাউন্ট থেকে প্রতারকের অ্যাকাউন্টে টাকা স্থানান্তর করতে পারে এবং এটিএম থেকে টাকা তুলতে পারে (প্রকৃত জালিয়াতি)।

উপরোক্ত প্রতারণা থেকে গ্রাহকদের রক্ষা করতে, ব্যাংকগুলোকে গ্রাহকের কম্পিউটার থেকে ব্যাংকের সার্ভারে ভ্রমণ করার সময় তাদের পাসওয়ার্ড চুরি হওয়া বা ফিশিং আক্রমণ থেকে রক্ষা করতে হবে। ব্যাংকগুলো ৩য় পক্ষের অ্যাকাউন্টে টাকা স্থানান্তর এবং এলসি ট্রান্সমিশনের জন্য একটি বাধ্যতামূলক '২-ফ্যাক্টর অথেনটিকেশন' পদ্ধতি চালু করতে পারে।

এই সুরক্ষা ব্যবস্থাগুলো সংক্ষেপে নিচে বর্ণিত হয়েছে।

**ক. গ্রাহকের পিসি থেকে ব্যাংক সার্ভারে ট্রান্সমিশনের সময় পাসওয়ার্ড ক্যাপচার করা—**

পাসওয়ার্ডটি গ্রাহকের কম্পিউটার থেকে ব্যাংকের সার্ভারে ইন্টারনেটের মাধ্যমে ভ্রমণ করার সময়, একজন জালিয়াতি সহজেই এটি ক্যাপচার করতে পারে এবং ইন্টারনেট ব্যাংকিং সিস্টেমে প্রবেশের জন্য তথ্যটি ব্যবহার করতে পারে। ভ্রমণের সময় পিনটি ক্যাপচার থেকে রক্ষা করতে, ব্যাংকের সিস্টেমটি অবশ্যই পিনটি এনক্রিপ্ট করে এবং সার্ভারে আনতে এবং পরবর্তী প্রক্রিয়াজাতকরণের আগে সেগুলো ডিক্রিপ্ট করতে সক্ষম হতে হবে। যদি কোনো প্রতারক পথে এনক্রিপ্ট করা তথ্য ক্যাপচার করে, তবে তার পক্ষে তা ডিক্রিপ্ট করে প্রকৃত পিন বের করা সম্ভব নয়। ফলে পথে পিনটি নিরাপদ।

**খ. ফিশিং (Phishing)**

ফিশিং হলো ব্যবহারকারীর কাছে একটি জাল ওয়েবসাইট উপস্থাপন করে


*ভেরিসাইন ওয়েবসাইটের ঠিকানা ব্যবহারকারীদের কাছে জানা উচিত*

ব্যবহারকারীর কাছ থেকে পিন সংগ্রহ করা। উদাহরণস্বরূপ, ধরা যাক, যে কোনো ব্যাংকের ওয়েবসাইটের ঠিকানা www.abc-bank.com। হ্যাকার ব্যাংকের ওয়েবসাইটের ঠিক অনুরূপ একটি জাল ওয়েবসাইট তৈরি করবে, এবং ধরা যাক, ওয়েবসাইটে www.abe-bank.com ঠিকানায় তা রাখা হয়েছে। এখন যদি কোনো ব্যবহারকারী গুগলে 'এবিসি' ব্যাংকের সন্ধান করে তবে এই জাল ওয়েবসাইটের ঠিকানাও অনুসন্ধান ফলাফলের মধ্যে প্রদর্শিত হবে। এখন যদি ব্যবহারকারী এই লিঙ্কটিতে ক্লিক করেন তবে তিনি জাল ওয়েবসাইটে যাবেন। যদি তিনি ওয়েবসাইটের ঠিকানাটি সাবধানতার সঙ্গে না দেখেন বা ঠিকানাটি তার জানা না থাকে তবে তিনি তার আইডি এবং পাসওয়ার্ডটি জাল ওয়েব-পৃষ্ঠায় প্রবেশ করবেন। হ্যাকার বিভিন্ন ব্যবহারকারীর দ্বারা করা এই জাতীয় সব প্রচেষ্টা রেকর্ড করবে এবং আইডি এবং পাসওয়ার্ড সংগ্রহ করবে।

ভুয়া ওয়েবসাইটের ঠিকানাটি বিভিন্ন ব্যবহারকারীর কাছে ইমেলের মাধ্যমে প্রেরণ করা যেতে পারে যেখানে কোনো ব্যাংকের নামে গ্রাহককে তার আই-ব্যাংকিং সিস্টেমে প্রবেশ করতে এবং কিছু পরীক্ষা করার জন্য অনুরোধ করা হবে। ব্যবহারকারীরা, যারা ফিশিং আকর্ষণ সম্পর্কে সচেতন নন, তারা তার আইডি এবং পাসওয়ার্ড ব্যবহার করে মিথ্যা ওয়েবসাইটে লগইন করার চেষ্টা করতে পারেন। এভাবে গ্রাহকের সমস্ত তথ্য হ্যাকারের ডাটাবেসে ক্যাপচার করা হবে।

হ্যাকার এখন আই-ব্যাংকিং সিস্টেমে প্রবেশ করতে এবং প্রতারণামূলক ক্রিয়াকলাপ করতে সংগৃহীত আইডি এবং পাসওয়ার্ড ব্যবহার করতে পারে।

গ্রাহকদের পক্ষে ব্যাংকের সঠিক ওয়েবসাইটের ঠিকানা জানা সম্ভব না-ও হতে পারে। সুতরাং আই-ব্যাংকিং সেবা প্রদানকারী ব্যাংকের ওয়েবসাইটটি 'VeriSign'–এর মতোন সার্টিফায়িং অথোরিটি দ্বারা প্রত্যয়িত করা যেতে পারে। গ্রাহকের আইডি এবং পাসওয়ার্ড সংগ্রহ করে ব্যাংকের এমন পৃষ্ঠাটি সার্টিফায়িং অথোরিটির সিল প্রদর্শন করবে। যদি কোনো গ্রাহক সিলটিতে ক্লিক করেন, তবে প্রত্যয়িত কর্তৃপক্ষের ওয়েবসাইটটি উপস্থিত হবে। গ্রাহকদের অবশ্যই প্রতিষ্ঠিত সার্টিফায়িং অথোরিটির ওয়েব ঠিকানা জানতে হবে এবং এভাবে এর সঠিকতা যাচাই করতে হবে। যদি সার্টিফায়িং অথোরিটির ওয়েবসাইট ঠিকানা সঠিক হয়, তবে ব্যাংকের ওয়েবসাইট পৃষ্ঠাও সঠিক বলে প্রমাণিত হয়। ফলে গ্রাহক এই ওয়েবপৃষ্ঠায় নিরাপদে আইডি এবং পাসওয়ার্ড প্রবেশ করাতে পারেন।

**গ. প্রত্যাখ্যান এবং ডিজিটাল স্বাক্ষর (Repudiation and Digital Signature)**

কখনও কখনও কিছু গ্রাহক ইন্টারনেট ব্যাংকিং সিস্টেমের মাধ্যমে ইন্টারনেটে কিছু ক্রিয়াকলাপ করেন এবং পরে তিনি এটি করেননি বলে অস্বীকার করেন। বরং তারা বলে যে ব্যাংক কর্মকর্তারা সিস্টেম থেকে তাঁর পাসওয়ার্ড জানতে পারে এবং তার অ্যাকাউন্ট থেকে অর্থ স্থানান্তর করার জন্য লেনদেনগুলো করতে পারে। এটি নিশ্চিত যে ব্যাংক অফিসারের গ্রাহকের পাসওয়ার্ডে কোনো অ্যাক্সেস নেই কারণ সমস্ত পাসওয়ার্ড যৌক্তিকভাবে এমন একটি সিস্টেমে রেকর্ড করা হয়েছে যেখানে কোনো ব্যাংক অফিসার এমনকি প্রশাসকেরও অ্যাক্সেস নেই। তদুপরি সিস্টেমে ইলেকট্রনিক রেকর্ড রয়েছে যা থেকে সহজেই সুবিধাভোগীর নাম এবং ঠিকানা সহ লেনদেনের ইতিহাস পাওয়া যেতে পারে এবং তা স্পষ্টভাবে ইঙ্গিত দেয় যে ব্যাংক কর্মকর্তা এই লেনদেনের কোনো সুবিধাভোগী নন। তবে গ্রাহকদের কাছে এটি বোঝানো খুব কঠিন হয়ে পড়ে। ডিজিটাল স্বাক্ষর এটির সমাধান।

ডিজিটাল স্বাক্ষরটি হলো প্রেরক কর্তৃক তার প্রাইভেট কী ব্যবহার করে কোনো একটি বার্তা বা লেনদেনকে স্বাক্ষর করা (বা এনক্রিপ্টিং) যা প্রাপক কেবলমাত্র প্রেরকের পাবলিক কী ব্যবহার করে খুলতে (বা ডিক্রিপ্ট করতে) পারে। পাবলিক ও প্রাইভেট কী একটি ইস্যুকারী কর্তৃপক্ষ (সাধারণত সরকারী কর্তৃপক্ষ, বাংলাদেশে এটি বাংলাদেশ কম্পিউটার কাউন্সিল ও বাংলাদেশ ব্যাংক) কর্তৃক ব্যবহারকারীর কাছে ইস্যু করা হয়। এরপরে ব্যবহারকারী তার পাবলিক কীটি অন্য ব্যবহারকারী বা প্রতিষ্ঠান যাদের সঙ্গে তিনি ইলেকট্রনিক তথ্য বিনিময় করতে চান (যেমন ইমেল বা ব্যাংকিং লেনদেনের মতো) তাদের সঙ্গে শেয়ার করেন এবং তার প্রাইভেট কীটি

তার সঙ্গে (তার কম্পিউটার বা পেন ড্রাইভে) রাখেন। এখন তিনি তার প্রাইভেট কী ব্যবহার করে সমস্ত সংবেদনশীল তথ্য এনক্রিপ্ট বা স্বাক্ষর করেন এবং অন্য পক্ষকে প্রেরণ করবেন। অন্য পক্ষ কেবল প্রেরণকারীর পাবলিক কী ব্যবহার করে ঐ তথ্য ডিক্রিপ্ট করতে সক্ষম হবে। এটি নিশ্চিত করে যে লেনদেনটি ব্যবহারকারী নিজেই পাঠিয়েছেন। যদি ব্যবহারকারী এই জাতীয় লেনদেন প্রত্যাখ্যান করে, আদালত আইসিটি আইন ২০০৬-এর ভিত্তিতে রায় দিতে পারে।

ব্যাংক এমন একটি সিস্টেম তৈরি করতে পারে, যা কেবল গ্রাহকের কাছ থেকে তার প্রাইভেট কী ব্যবহার করে এনক্রিপ্ট করা লেনদেনের অনুরোধ গ্রহণ করবে। সমস্ত গ্রাহক যারা আই-ব্যাংকিং ব্যবহার করে তহবিল স্থানান্তর করতে ইচ্ছুক, তাদেরকে ব্যাংক ইস্যুকারী কর্তৃপক্ষের কাছ থেকে পাবলিক ও প্রাইভেট কী সংগ্রহ করতে এবং তার পাবলিক কী টি ব্যাংকে জমা দেওয়ার জন্য অনুরোধ করা হবে।

### ঘ. টু-ফেক্টর অথেনটিকেশন (Two-Factor Authentication)

পাসওয়ার্ড হ্যাকার দ্বারা হ্যাক হতে পারে এবং ইন্টারনেট ব্যাংকিং সিস্টেমে অননুমোদিত লেনদেন করার জন্য ব্যবহার করতে পারে। এই জাতীয় লেনদেনগুলো সুরক্ষিত করার জন্য, টু-ফ্যাক্টর অথেনটিকেশন প্রবর্তন করতে পারে, যার অর্থ কোনো গ্রাহককে দুটি 'ফেক্টর' ব্যবহার করে একটি লেনদেন করতে হবে—একটি পাসওয়ার্ড এবং অন্যটি একটি টোকেন যাকে বলা হয় ক্রিপ্টোগ্রাফিক বা USB বা হার্ডওয়্যার টোকেন।

একটি টোকেন হলো একটি ছোট হার্ডওয়্যার, যা ব্যাংক কর্তৃক গ্রাহককে প্রদান করা হয়। ডিভাইস ও অথেনটিকেশন সার্ভারে অবস্থিত টোকেন অ্যালগরিদম একই রকম, ফলে সার্ভার এবং টোকেন উভয়ই প্রতিটি নির্দিষ্ট সময়কালের পরে একই সংখ্যা তৈরি করে (যেমন ১ মিনিট পর পর)। আইডি এবং পাসওয়ার্ড টাইপ করার পরে, ব্যবহারকারী ইন্টারনেট ব্যাংকিং সিস্টেমে অ্যাক্সেস পান। তৃতীয় 'পার্টি' তহবিল স্থানান্তর বা এলসি প্রেরণ


*ইউএসবি টোকেন*

করার সময় গ্রাহককে সেই নির্দিষ্ট সময়ে তার টোকেনে প্রদর্শিত নম্বরটি প্রবেশ করতে বলা হয়। তিনি তার টোকেন থেকে নম্বরটি সংগ্রহ করে তা সিস্টেমে ইনপুট দেন। ইন্টারনেট ব্যাংকিং সিস্টেম এই টোকেন নম্বরটি টোকেন আইডি অথেনটিকেশন সার্ভারে প্রেরন করে যা সংখ্যার যথার্থতা পরীক্ষা করে। যদি নম্বরটি সঠিক হয় তবে লেনদেনটি পাস হয়, অন্যথায় প্রত্যাখ্যান করা হয়।

যেহেতু টোকেনটি একটি হার্ডওয়্যার ডিভাইস যা ব্যবহারকারীর অন্তর্গত এবং রেনডম নম্বর উৎপন্ন করে, হ্যাকার এটি ক্যাপচার করতে পারে তবে পরবর্তী মুহূর্তেই তা অবৈধ হয়ে উঠবে। এইভাবে টু-ফ্যাক্টর অথেনটিকেশন গ্রাহকদের আরও বেশি সুরক্ষা প্রদান করে। টোকেন যেহেতু গ্রাহকের কাছে থাকে, তাই গ্রাহকের দ্বারা লেনদেন প্রত্যাখ্যান করার সুযোগ নেই।

## ৭. এসএমএস এবং অ্যালার্ট ব্যাংকিং

### ৭.১. এসএমএস ব্যাংকিং (SMS Banking)

এসএমএস ব্যাংকিং হলো গ্রাহকের নিবন্ধিত মোবাইল ডিভাইস থেকে এসএমএস প্রেরণ করে কিছু ব্যাংকিং কার্যক্রম সম্পাদনের একটি উপায়। এটি একটি পোশ ও পোল পরিষেবা। গ্রাহকের অবশ্যই একটি ডিপোজিট অ্যাকাউন্ট থাকতে হবে এবং তার মোবাইল নম্বর অবশ্যই অ্যাকাউন্টের সঙ্গে লিঙ্ক করা থাকতে হবে। গ্রাহকের অনুরোধে, একজন ব্যাংক অফিসার গ্রাহকের অ্যাকাউন্টকে প্রদত্ত মোবাইল নম্বরের সঙ্গে লিঙ্ক করে। গ্রাহককে একটি পিন দেওয়া হয়, যা তিনি সমস্ত লেনদেনের সময় ব্যবহার করবেন। প্রতিটি মেসেজের একটি প্রাক-সংজ্ঞায়িত সিনট্যাক্স রয়েছে। গ্রাহককে অবশ্যই সিনট্যাক্স অনুযায়ী এসএমএস প্রেরণ করতে হবে। উদাহরণস্বরূপ, যদি ব্যালেন্স চেক করার সিনট্যাক্সটি 'Bal <PIN>' হয় এবং পিনটি ১২৩৪ হয় তবে গ্রাহককে অবশ্যই এসএমএস লিখতে হবে: 'Bal 1234' এবং ব্যাংকের শর্ট কোডে তাহা প্রেরণ করতে হবে। যদি ব্যাংকের শর্ট কোডটি ৩২২৫ হয় তবে এসএমএস ৩২২৫ এ প্রেরণ করতে হবে। ব্যাংক থেকে ফিরতি এসএমএসের মাধ্যমে গ্রাহককে তার অ্যাকাউন্টের ব্যালেন্স জানানো হবে। সিনট্যাক্স এবং কিছু এসএমএস ফাংশনের উদাহরণ নিচে দেওয়া

হয়েছে—

- ব্যালেন্স চেক করা
  —সিনট্যাক্স : Bal <PIN>
  —উদাহরণ : Bal 1234
- স্টেইটম্যান্ট দেখা
  —সেন্টাক্স : STM <PIN>
  —উদাহরণ : STM 1234
- পোস্ট-পেইড মোবাইলের বিল পরিশোধ করা
  —সেন্টাক্স : PAY <PIN> <Amount> <Mobile#>
  —উদাহরণ : PAY 1234 100 01911223344
  —ব্যাখ্যা : যদি মোবাইল # অন্তর্ভুক্ত না করা হয় তবে যে মোবাইল থেকে এসএমএস প্রেরণ করা হয়েছে, সেই মোবাইলের বিল পরিশোধ করা হবে।
- প্রি-পেইড মোবাইলে টাকা ঢোকানো—
  —সিনট্যাক্স : RFL <PIN> <Amount> <Mobile #>
  —উদাহরণ : RFL 1234 100 01911223344
  —ব্যাখ্যা : যদি মোবাইল # অন্তর্ভুক্ত না করা হয় তবে যে মোবাইল থেকে এসএমএস প্রেরন করা হয়েছে, সেই মোবাইলে টাকা রিফিল করা হবে।
- পিন পরিবর্তন
  —সিনট্যাক্স : PIN <Old PIN> <New PIN>
  —উদাহরণ : PIN 1234 4321
- ইউটিলিটি বিল পেমেন্ট
  —সিনট্যাক্স : UTL <পিন> <অ্যামাউন্ট> <কোম্পানি কোড> <অ্যাকাউন্ট# / গ্রাহক# / টেলিফোন# / মিটার#>
  —উদাহরণ : UTL ১২৩৪ ১০০ ১০১ ১.১১২৩৪৫৬

> ব্যাখ্যা: প্রতিটি ইউটিলিটি কোম্পানির জন্য ইউনিক কোম্পানি কোড ব্যাংক দ্বারা প্রকাশিত হয়

- শপিং বিল পেমেন্ট
  —সিনট্যাক্স : POS <PIN> <Amount> <Merchant Code>
  —উদাহরণ : POS 1234 100 301
  —ব্যাখ্যা : প্রতিটি ব্যবসায়ীর জন্য ব্যাংক দ্বারা একটি অনন্য মার্চেন্ট কোড প্রকাশিত হয়।

### ৭.২. অ্যালার্ট ব্যাংকিং (Alert Banking)

অ্যালার্ট ব্যাংকিং একটি পুশ পরিষেবা, তাই গ্রাহককে অ্যালার্টের জন্য কিছু করতে হয় না। কিন্তু, তাকে অ্যালার্ট পরিষেবার জন্য ব্যাংকে তার মোবাইল নম্বর নিবন্ধন করতে হবে এবং ব্যাংক এই পরিষেবার জন্য একটি ফি নিতে পারে।

অ্যালার্ট ব্যাংকিং সিস্টেম, অ্যালার্ট এসএমএস গ্রাহকের মোবাইলে পাঠায়। সিস্টেমটি প্রথমে ব্যাংকের শর্টকোডে এসএমএস পাঠায়। সংশ্লিষ্ট মোবাইল অপারেটরের সিস্টেম এসএমএস পেয়ে তা গ্রাহকের মোবাইলে প্রেরণ করে।
সিস্টেমটি তিন ধরনের অ্যালার্ট তৈরি করে—ডেবিট অ্যালার্ট, ক্রেডিট অ্যালার্ট এবং পিরিয়ডিক অ্যালার্ট। তিন ধরনের অ্যালার্ট নিচে সংজ্ঞায়িত করা হয়েছে—

#### ৭.২.১. ডেবিট অ্যালার্ট (Debit Alert)

গ্রাহক তার মোবাইলে স্বয়ংক্রিয়ভাবে তৈরি একটি অ্যালার্ট এসএমএস পাবেন, যখন তার অ্যাকাউন্টে নির্দিষ্ট পরিমাণের চেয়ে বেশি পরিমাণের জন্য ডেবিট করা হয়। গ্রাহক নিবন্ধনের সময় ঐ পরিমাণ উল্লেখ করে থাকেন। সাধারণত সেটি শূন্য টাকা হয়।

#### ৭.২.২. ক্রেডিট অ্যালার্ট (Credit Alert)

গ্রাহক তার মোবাইলে স্বয়ংক্রিয়ভাবে তৈরি একটি অ্যালার্ট পাবেন, যখন তার অ্যাকাউন্টে নির্দিষ্ট পরিমাণের চেয়ে বেশি পরিমাণে টাকা জমা হয়। গ্রাহক নিবন্ধনের সময় ঐ পরিমাণ উল্লেখ করে থাকেন।

#### ৭.২.৩. পিরিয়ডিক অ্যালার্ট (Periodic Alert)

মাসের শেষে অ্যাকাউন্টের ব্যালেন্স বা অন্য কোনো তথ্য পাঠানোর জন্য পিরিয়ডিক অ্যালার্ট তৈরি করা হয়। ব্যাংক কর্মকর্তারা এই ধরনের পিরিয়ডিক অ্যালার্ট-এর সূচনা করে থাকেন।

### ৭.৩. এসএমএস ব্যাংকিং কীভাবে কাজ করে?

ব্যাংক তার ডেটা সেন্টারে এসএমএস/অ্যালার্ট ব্যাংকিংয়ের জন্য সফ্টওয়্যার ইনস্টল করে এবং কোর ব্যাংকিং সিস্টেমের সঙ্গে এসএমএস/ অ্যালার্ট ব্যাংকিং সিস্টেমের একটি ইন্টারফেস তৈরি করে। ব্যাংক মোবাইল অপারেটরদের সঙ্গে একটি সংযোগ স্থাপন করে এবং টেক্সট মেসেজ পাঠানো ও গ্রহণ করার জন্য প্রয়োজনীয় ব্যবস্থা গ্রহণ করে। মোবাইল অপারেটর ব্যাংকের জন্য একটি সংক্ষিপ্ত কোড বরাদ্দ করবে, যেমন ৩২২৫।

এখন গ্রাহক ব্যাংক দ্বারা সংজ্ঞায়িত সিনট্যাক্স অনুসারে এসএমএস টাইপ করে (যেমন, BAL ১২৩৪) এবং শর্ট কোডে পাঠায়। এসএমএসটি মোবাইল

অপারেটরের এসএমএস সার্ভারে যাবে। মোবাইল অপারেটর যে মোবাইল নম্বর থেকে এসএমএস তৈরি করা হয়েছে তা টেক্সটের সঙ্গে যোগ করবে (০১৯১১২২৩৩৪৪ BAL ১২৩৪) এবং সংযোগের মাধ্যমে পুরো টেক্সটটি ব্যাংকের এসএমএস/ অ্যালার্ট সফ্টওয়্যারে পাঠায়।

ব্যাংকের এসএমএস/ অ্যালার্ট সফ্টওয়্যার তখন নিম্নলিখিত কাজ করবে—

ক. পাসওয়ার্ড (১২৩৪) সঠিক কিনা তা পরীক্ষা করা।

খ. পাসওয়ার্ড সঠিক না হলে গ্রাহকের মোবাইলে 'ভুল পাসওয়ার্ড' বার্তা পাঠানো হবে। পাসওয়ার্ডটি সঠিক হলে, সিস্টেমটি এই মোবাইল নম্বরের সঙ্গে নিবন্ধনের সময় লিঙ্ক করা অ্যাকাউন্ট নম্বরটি খুঁজে বের করবে।

গ. BAL কীওয়ার্ড থেকে ব্যাংকের এসএমএস/ অ্যালার্ট সিস্টেম বুঝতে পারবে যে গ্রাহক তার অ্যাকাউন্টের ব্যালেন্স জানতে চান।

ঘ. এসএমএস/ অ্যালার্ট ব্যাংকিং সিস্টেম কোর ব্যাংকিং সিস্টেমে গ্রাহকের অ্যাকাউন্ট নম্বর পাঠায় এবং ঐ অ্যাকাউন্টের বর্তমান ব্যালেন্সের পরিমাণ ফেরত পাঠানোর জন্য অনুরোধ করে।

ঙ. কোর ব্যাংকিং সিস্টেম বর্তমান ব্যালেন্স খুঁজে বের করবে এবং এসএমএস/ অ্যালার্ট ব্যাংকিং সিস্টেমে পাঠাবে।

চ. এসএমএস/অ্যালার্ট ব্যাংকিং সিস্টেম ব্যালেন্সের পরিমাণ ব্যবহার করে একটি এসএমএস তৈরি করবে, যেমন 'তারিখ: ২০/১০/২০১০; সময়: ২২:২৩; অ্যাকাউন্ট নম্বর: ৯৯৯৯৯৯৯৯; ব্যালেন্স: ৯৯৯৯.৯৯ টাকা' এবং এটিকে গ্রাহকের মোবাইলে ফেরত পাঠাবে।

### ৭.৪. গ্রাহকদের জন্য গুরুত্বপূর্ণ নির্দেশনা

১. অনুগ্রহ করে এসএমএস পিন মুখস্থ করুন এবং পিন মেইলারটি ছিঁড়ে ফেলুন/মুছে ফেলুন।

২. কাউকে এসএমএস পিন শেয়ার করবেন না।

৩. গ্রাহক ঘন ঘন তার পিন পরিবর্তন করা ভালো।

৪. যেহেতু গ্রাহকের পাঠানো এসএমএসে তার পিন থাকে, তাই সুপারিশ করা হয় যে গ্রাহক তার 'Send Item' বা 'আউটবক্স' থেকে এসএমএসটি অবিলম্বে মুছে ফেলবেন।

৫. যৌথভাবে তার পিন এবং মোবাইলের অপব্যবহারের কারণে গ্রাহকের অ্যাকাউন্টে কোনো প্রতারণামূলক কার্যকলাপের জন্য ব্যাংকগুলো দায়ী থাকবে না।

### ৭.৫. এসএমএস এবং অ্যালার্ট ব্যাংকিংয়ে নিরাপত্তা

এসএমএস ব্যাংকিং এ ব্যবহৃত কমান্ড এবং তথ্য গ্রাহকের মোবাইল ডিভাইস থেকে 'শর্ট মেসেজিং সিস্টেম' ব্যবহার করে ব্যাংকের সার্ভারে পাঠানো হয়, যা একটি সাধারণ টেক্সট। মোবাইল এবং সার্ভারের মধ্যে কোনো এনক্রিপশন নেই। এটি সেশনভিত্তিকও নয়। ফলে এসএমএস ব্যাংকিং সুরক্ষিত নয়।

অন্যদিকে, এসএমএস একটি 'স্টোর এবং ফরওয়ার্ড ডেটা' পরিষেবা। ফলে পিনসহ মেসেজের পুরো লেখা মোবাইল সেটে জমা থাকে। মুছে ফেলা না হলে, এটি অন্য লোকেদের কাছে প্রকাশ পেয়ে যেতে পারে।

তাই এসএমএস ব্যাংকিং ব্যবহার করে কোনো ফান্ড ট্রান্সফার লেনদেনের অনুমতি দেওয়া বাঞ্ছনীয় নয়।

## ৮. ই-কমার্স ও ইন্টারনেট পেমেন্ট গেটওয়ে

### ৮.১. ই-কমার্স (e-commerce)

ইন্টারনেটের মাধ্যমে পণ্য ও সেবা ক্রয়-বিক্রয়কে ই-কমার্স বলে। ই-মার্চেন্টদের একটি শহরের বিশিষ্ট স্থানে দোকান স্থাপনের প্রয়োজন নেই। তাদের কাছে কেবল গুদামঘর থাকবে, যেখান থেকে তারা সহজেই গ্রাহকের ঠিকানায় পণ্য সরবরাহ করতে পারে। গ্রাহকরা অনলাইনে অর্ডার দেবেন এবং অনলাইনে বিল পরিশোধ করবেন। ব্যবসায়ী সংশ্লিষ্ট আইটেমের জন্য ওয়েবসাইটে ঘোষিত সময়ের মধ্যে পণ্য সরবরাহ করবে। একটি ভালো ই-কমার্স ওয়েবসাইটের প্রয়োজনীয়তাগুলো নিচে দেওয়া হলো—

- সাইটটি বিক্রি করা সমস্ত আইটেমের পরিষ্কার ছবি প্রদর্শন করে থাকে।
- ছবিগুলোর সঙ্গে বিস্তারিত স্পেসিফিকেশন, আকার, ক্ষমতা ইত্যাদির যুক্ত করা উচিত।
- প্রতিটি আইটেমের দাম।
- ওয়ারেন্টি, যদি প্রযোজ্য হয়।
- ডেলিভারি সময়কাল (স্থান অনুযায়ী ভিন্ন হতে পারে)।
- এই মুহূর্তে দ্রব্যটির প্রাপ্যতার পরিমাণ।
- গ্রাহকদের নিবন্ধনের সুবিধা।
- সাইটটি অত্যন্ত সুরক্ষিত হওয়া উচিত।

ইন্টারনেট একটি নতুন অর্থনৈতিক ইকোসিস্টেম তৈরি করেছে যা হলো, ই-কমার্স মার্কেটপ্লেস। ই-কমার্স আঞ্চলিক এবং বিশ্বব্যাপী পণ্য এবং পরিষেবা বিনিময়ের একটি দ্রুত এবং সুবিধাজনক উপায় প্রদান করে দিন দিন বৃদ্ধি পেয়েছে। বর্তমানে,

ই-কমার্স একটি বিশাল শিল্পে পরিণত হয়েছে যেখানে মার্কিন অনলাইন বিক্রেতারা ২০০৭ সালে ১৭৫ বিলিয়ন ডলার আয় করেছে। বি টু সি অনলাইন লেনদেনগুলো ভ্রমণ পরিষেবা থেকে ভোক্তা ইলেকট্রনিক্স, বই এবং মিডিয়া বিতরণ থেকে খেলাধুলা এবং ফিটনেস পর্যন্ত শিল্পগুলোকে প্রভাবিত করছে।

এটি লক্ষ করা গুরুত্বপূর্ণ যে বেশিরভাগ ই-কমার্স প্লেয়ার খুচরা বিক্রেতাদের তুলনায় একটি প্রতিযোগিতামূলক সুবিধাতে রয়েছে। ভার্চুয়াল কমার্স পরিবেশে কাজ করার কারণে তাদের কম অপারেটিং খরচ এবং ভালো ইনভেন্টরি ম্যানেজমেন্ট রয়েছে। উদাহরণস্বরূপ, amazon.com-এর প্রতি কর্মচারীর আয় প্রায় ৮৫০,০০০ ডলার, যেখানে এর রিটেইল প্রতিপক্ষ, বেস্ট বাই এর কর্মচারী প্রতি আয় মাত্র ২৭০,০০০ ডলার।

### ৮.২. ইন্টারনেট পেমেন্ট গেটওয়ে (Internet Payment Gateway)

একটি ই-কমার্সের নিম্নরূপ একটি জীবনচক্র রয়েছে—

১. ব্যবসায়ীরা (বিক্রেতারা) তাদের কোম্পানি, পণ্য এবং ডেলিভারি প্রতিশ্রুতি সম্পর্কে বিস্তারিত তথ্য প্রদান করবে—যাতে গ্রাহক তাদের পণ্য সম্পর্কে জানতে পারে। এটি একটি ওয়েবসাইটের মাধ্যমে করা যেতে পারে।

২. গ্রাহক ওয়েবপৃষ্ঠাগুলোর মাধ্যমে পণ্য বেছে নেয় এবং অর্ডার প্রদান করে।

৩. গ্রাহক ব্যাংকের পেমেন্ট গেটওয়ের মাধ্যমে তার ক্রেডিট/ডেবিট কার্ডের ব্যবহার করে পেমেন্ট করেন।

৪. হোম সার্ভিস বা ডাক/কুরিয়ার সার্ভিসের মাধ্যমে গ্রাহকের কাছে পণ্য সরবরাহ করা হয়। বিক্রেতার উচিত সময়মতো ডেলিভারি করা এবং পণ্যের গুণগত মান নিশ্চিত করা।

৫. ওয়ারেন্টি সময়কালে সেবা সরবরাহ করা (যদি প্রযোজ্য হয়)।

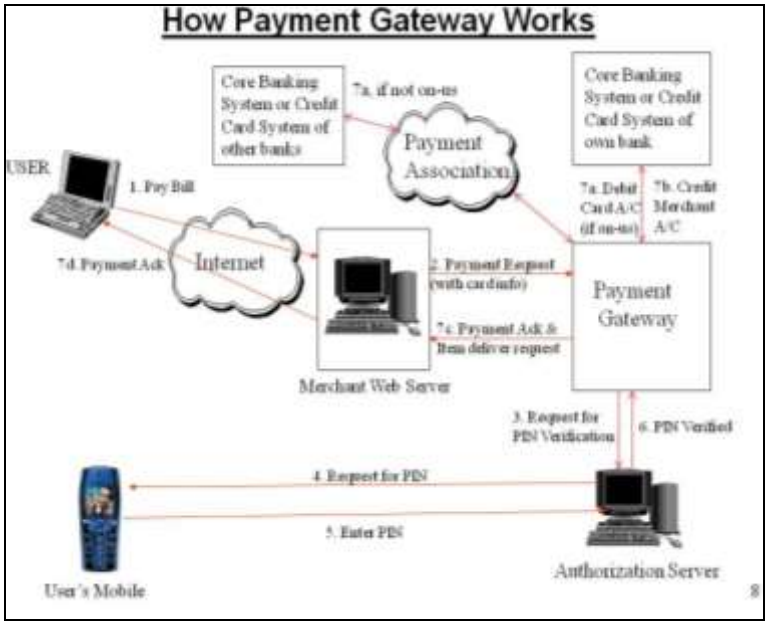
ব্যাংক ওপরের বর্ণিত ৩ নং পর্যায়ে অংশগ্রহণ করে। গ্রাহকের কার্ড অ্যাকাউন্ট (ব্যাংক-A তে অবস্থিত) থেকে মার্চেন্টের ব্যাংক অ্যাকাউন্টে (ব্যাংক-B বা A তে অবস্থিত) অর্থপ্রদানের পরিমাণ স্থানান্তর করার জন্য, ব্যাংক জড়িত। এই ধরনের তহবিল স্থানান্তর কার্যকর করার জন্য, ব্যাংক তার ডেটা সেন্টারে একটি বিশেষ সফ্টওয়্যার ইনস্টল করে। এই সফ্টওয়্যারটির সঙ্গে মার্চেন্টের ওয়েবসাইট, ব্যাংকের কোর ব্যাংকিং সিস্টেম, ক্রেডিট কার্ড সিস্টেম এবং কার্ড অ্যাসোসিয়েশনগুলোর সঙ্গে (যেমন ভিসা ও মাস্টারকার্ড) একটি লিঙ্ক রয়েছে।

তাই একটি ইন্টারনেট পেমেন্ট গেটওয়েকে এভাবে সংজ্ঞায়িত করা যেতে পারে যে, এটি একটি সফ্টওয়্যার যা একটি ব্যাংক তার ডেটা সেন্টারে ইনস্টল করে যাতে কার্ডধারীদের দ্বারা ই-মার্চেন্টদের করা অর্থপ্রদান সহজে প্রক্রিয়াকরণ করা যায়।

### ৮.৩. ইন্টারনেট পেমেন্ট গেটওয়ে কীভাবে কাজ করে?

একটি ওয়েবসাইট থেকে ক্রয় করা আইটেম নির্বাচন করার পরে, গ্রাহক মার্চেন্টের ওয়েবসাইটে 'চেক আউট' বা 'পে' বোতামে ক্লিক করেন। এই বোতামটিতে একটি কম্পিউটার কোড রয়েছে, যা API নামে ব্যাংক সরবরাহ করে এবং যা ক্লিক করলে একটি ব্যাংকের পৃষ্ঠা কল করা হয়। এই পৃষ্ঠায়, গ্রাহককে তার কার্ডের তথ্য প্রদান করতে হয় যেমন কার্ড নম্বর, পিন/সিভিভি/সিভিসি, মেয়াদ শেষ হওয়ার তারিখ ইত্যাদি। PIN বলতে পার্সোনাল আইডেন্টিফিকেশন নাম্বার, CVV বলতে কার্ড ভ্যারিফিকেশন ভ্যালু বোঝায়, যা ভিসা ব্যবহার করে থাকে এবং CVC বলতে কার্ড ভেরিফিকেশন কোড বোঝায় যা মাস্টার কার্ড ব্যবহার করে থাকে। মূল্য স্বয়ংক্রিয়ভাবে পৃষ্ঠায় প্রদর্শিত হবে। এই তথ্যগুলো নিরাপদ উপায়ে ব্যাংকের ইন্টারনেট পেমেন্ট গেটওয়ে সফ্টওয়্যারে প্রেরণ করা হয়।

ইন্টারনেট পেমেন্ট গেটওয়ে সঠিকতার জন্য তথ্য পরীক্ষা করে। যদি সরবরাহ করা তথ্য সঠিক পাওয়া যায়, সিস্টেমটি ক্রেতাদের ব্যাংক বা কার্ড অ্যাকাউন্ট ডেবিট করে এবং মার্চেন্টের অ্যাকাউন্টে ক্রেডিট করে। তারপর সিস্টেম উভয় পক্ষকে কর্ম সম্পাদন সম্পর্কে অবহিত করে।




*পেমেন্ট গেটওয়ে কীভাবে কাজ করে*

যদি কার্ডটি একই ব্যাংকের না হয়, তাহলে পেমেন্ট গেটওয়ে নির্ধারিত পেমেন্ট অ্যাসোসিয়েশনের কাছে তথ্য পাঠায় (মাস্টারকার্ড, ভিসা, এমেক্স, জেবিসি, ডিনার, ডিসকভার, ইত্যাদির নেটওয়ার্ক)। পেমেন্ট অ্যাসোসিয়েশন তারপর কার্ডের তথ্য ইস্যুকারী ব্যাংকে পাঠায়। ইস্যুকারী ব্যাংক হলো সেটি যা গ্রাহককে কার্ড ইস্যু করেছে।

এখন ইস্যুকারী ব্যাংক কার্ডের তথ্য যাচাই করে এবং যদি এটি সঠিক পাওয়া যায়, তবে ক্রেতার ব্যাংক অ্যাকাউন্ট বা কার্ড অ্যাকাউন্ট ডেবিট করে এবং এইভাবে লেনদেন অনুমোদন করে। অনুমোদনের বার্তাটি অ্যাকুয়ারিং ব্যাংকে যায় যা অতঃপর মার্চেন্টের অ্যাকাউন্টে ক্রেডিট করে এবং উভয় পক্ষকে পদক্ষেপ সম্পর্কে অবহিত করে।

যে উপায়ে অধিগ্রহণকারী ব্যাংক ইস্যুকারী ব্যাংকের কাছ থেকে অর্থ পায়, যদি ব্যাংক দুটি আলাদা হয়, তবে তাকে নিষ্পত্তি বা সেটেলম্যান্ট বলা হয়। পেমেন্ট অ্যাসোসিয়েশনগুলো ইস্যুকারী ব্যাংকের নস্ট্রো অ্যাকাউন্ট ডেবিট করে এবং অ্যাকুয়ারিং ব্যাংকের নস্ট্রো অ্যাকাউন্টে ক্রেডিট করে প্রতিদিন নিষ্পত্তি বা সেটেলম্যান্ট করে থাকে।

গৃহীত পদক্ষেপ সম্পর্কে অ্যাকুয়ারিং ব্যাংক থেকে প্রাপ্ত তথ্যের ওপর নির্ভর করে, মার্চেন্ট ক্রেতাদের ঠিকানায় পণ্য এবং পরিষেবা সরবরাহ করে।

উপরোক্ত লেনদেন প্রবাহের নিরাপত্তা কার্ডের তথ্য এবং/অথবা পিনের ওপর নির্ভর করে। লেনদেনকে আরও সুরক্ষিত করতে, কিছু ব্যাংক টু-ফেক্টর অথেনটিকেশন পদ্ধতি চালু করে। গ্রাহক ব্যাংক থেকে প্রাপ্ত তার USB টোকেন থেকে তৎক্ষণাৎ প্রদর্শিত কোডটি পেমেন্ট গেটওয়ের পৃষ্ঠায় এন্ট্রি দেন। একটি IVR কল ব্যবহার করে টু-ফেক্টর অথেনটিকেশন পদ্ধতিটির বর্ণনা নিচে প্রদত্ত হয়েছে।

একটি মোবাইল ডিভাইস ব্যবহার করে টু-ফেক্টর অথেনটিকেশন ওপরের চিত্রে দেখানো হয়েছে। গ্রাহকের অ্যাকাউন্ট ডেবিট করার আগে এবং মার্চেন্টের অ্যাকাউন্টে ক্রেডিট করার আগে, পেমেন্ট গেটওয়ে গ্রাহকের সত্যতা যাচাই করার জন্য একটি অথোরাইজেশন সার্ভারের কাছে অনুরোধ পাঠাবে। অথোরাইজেশন সার্ভার, একটি IVR এর মাধ্যমে, গ্রাহকের মোবাইলে একটি ভয়েস কল শুরু করে (আগে নিবন্ধিত) এবং পিনের জন্য অনুরোধ করে। গ্রাহক তার অ্যাকাউন্ট থেকে

ডেবিটের পরিমাণ এবং মার্চেন্টের নাম শোনেন এবং সঠিক পাওয়া গেলে মোবাইল ডিভাইসের কীপ্যাডে তার পিন টাইপ করেন। অথোরাইজেশন সার্ভার পিনটি যাচাই করে এবং সঠিক পাওয়া গেলে, ডেবিট এবং ক্রেডিট অনুরোধটি তার নিজস্ব হোস্টের কাছে পাঠায় (যদি অন-আস লেনদেন হয়) বা পেমেন্ট অ্যাসোসিয়েশনের নেটওয়ার্কে (যদি অফ-আস লেনদেন হয়) পাঠায়।

### ৮.৪. পেমেন্ট গেটওয়ে হিসাবে পেপাল

পেপ্যাল সাম্প্রতিক বছরগুলোতে অনলাইন পেমেন্টের অন্যতম জনপ্রিয় পদ্ধতিতে পরিণত হয়েছে। হাজার হাজার ব্যবসা পেপ্যাল পেমেন্ট গ্রহণ করে। যদি একজন গ্রাহক পেপ্যালের সঙ্গে যুক্ত এমন একটি মার্চেন্ট ওয়েবসাইট থেকে পণ্য এবং পরিষেবা ক্রয় করেন, তবে তিনি যে কোনো পেমেন্ট অ্যাসোসিয়েশনের কার্ড ব্যবহার করে অর্থ প্রদান করতে পারেন। যদি গ্রাহক আগে নিবন্ধিত হয়ে থাকে, তবে তাকে মার্চেন্ট ওয়েবসাইটে কার্ড বা ব্যাংক অ্যাকাউন্ট-সম্পর্কিত তথ্য দেওয়ার প্রয়োজন নেই, তবে তিনি শুধু পেপাল অ্যাকাউন্ট নম্বর সন্নিবেশ করবেন। ফলে গ্রাহকের কার্ড বা ব্যাংকের তথ্য অনেক অজানা জায়গায় উন্মোচিত হয় না।

লেনদেন সম্পন্ন করার জন্য গ্রাহককে পেপ্যালের সদস্য হওয়া বাধ্যতামূলক নয়। বহুমুখিতা (versatility) হলো পেপ্যাল পেমেন্ট প্রদানকারী হিসাবে জনপ্রিয় হওয়ার অন্যতম কারণ। লেনদেনগুলো সুরক্ষিত এবং পেপ্যাল অর্থপ্রদানের অপশনগুলো সেট আপ করা এবং সংযোক্ত করা সহজ।

পেপ্যাল ব্যবহারকারীদের প্রধান অভিযোগগুলোর মধ্যে একটি হলো বিরোধ নিষ্পত্তির ক্ষেত্রে গ্রাহকদের অসন্তোষটি। এছাড়াও কিছু পেপ্যাল পেমেন্টের ক্ষেত্রে 'রিফান্ড' পাওয়ার প্রক্রিয়া খুবই কঠিন।

### ৮.৫. ই-কমার্স লেনদেনের সময় জালিয়াতি এবং প্রতিকার

ই-কমার্সের সব লেনদেন ইন্টারনেটের ওপর নির্ভরশীল। ইন্টারনেট একটি পাবলিক সাইট। ইন্টারনেট ব্যবহার করে কার্ডের তথ্যের আদান-প্রদান নিরাপদ নয়। সুতরাং গ্রাহকের কম্পিউটার থেকে ব্যাংকের সার্ভারে লেনদেনের প্রবাহকে নিরাপদ করতে ব্যাংককে অবশ্যই পর্যাপ্ত ব্যবস্থা নিতে হবে। এই ব্যবস্থাগুলো সংক্ষেপে নিচে বর্ণিত হয়েছে।

#### ক. ব্যাংক সার্ভারে ট্রান্সমিশনের সময় কার্ডের তথ্য ক্যাপচার করা

কার্ডের তথ্য গ্রাহকের কম্পিউটার থেকে ব্যাংকের সার্ভারে ইন্টারনেটের মাধ্যমে ভ্রমণ করার সময়, একজন প্রতারক সহজেই তা ক্যাপচার করতে পারে এবং ঐ তথ্য ব্যবহার করে ইন্টারনেটে মূল্যবান পণ্য কিনতে বা ক্যাপচার করা তথ্য ব্যবহার করে একটি জাল কার্ড তৈরি করতে পারে এবং এটিএম থেকে টাকা তুলতে পারে। ফলে গ্রাহকের কাছ থেকে কার্ডের তথ্য ক্যাপচার করার সময়, ব্যাংকের সিস্টেম এটিকে তাৎক্ষণিকভাবে এনক্রিপ্ট করে এবং সার্ভারে আনে। পরবর্তী প্রক্রিয়াকরণের আগে সেগুলো ডিক্রিপ্ট করতে হবে। যদি একজন প্রতারক পথে

এনক্রিপ্ট করা তথ্য ক্যাপচার করে তবে তার পক্ষে ডিক্রিপ্ট করা এবং আসল তথ্য খুঁজে পাওয়া সম্ভব নয়। ফলে তথ্যের আদান-প্রদান নিরাপদ হয়।

**খ. ফিশিং (Phishing)**

ফিশিং হলো ইন্টারনেট ব্যবহারকারীর কাছে একটি জাল ওয়েবসাইট ঠিকানা উপস্থাপন করে ব্যবহারকারীর তথ্য সংগ্রহ করা। উদাহরণস্বরূপ, ধরা যাক আগোরা (একজন মার্চেন্ট) এর ওয়েবসাইটের ঠিকানা হলো www.agorabd.com। হ্যাকার আগোরার ওয়েবসাইটের অনুরূপ একটি ভুয়া ওয়েবসাইট তৈরি করবে, তবে একটি ভিন্ন ঠিকানা যেমন www.agora-bd.com ব্যবহার করে তা ইন্টারনেটে স্থান দেবে। এখন কোনো ক্রেতা গুগলে 'আগোরা' সার্চ করলে সার্চ রেজাল্টে এই ভুয়া ওয়েবসাইটের ঠিকানাও দেখা যাবে। এখন ক্রেতা এই লিঙ্কে ক্লিক করলেই সে ভুয়া ওয়েবসাইটে চলে যাবে। যদি তিনি ওয়েবসাইটের ঠিকানাটি মনোযোগ সহকারে না দেখেন বা ঠিকানাটি তার জানা না থাকে তবে তিনি পণ্য নির্বাচন করবেন এবং কার্ডের তথ্য এবং পিন ভুয়া ওয়েব পেজে প্রবেশ করবেন। হ্যাকার এভাবে বিভিন্ন ব্যবহারকারীদের কার্ডের তথ্য সংগ্রহ করবে।

তাছাড়া ভুয়া ওয়েবসাইটের ঠিকানা ইমেলের মাধ্যমে বিভিন্ন ব্যবহারকারীদের কাছে পাঠানো হতে পারে যেখানে আগোরার নামে অনেক লোভনীয় অফারও থাকতে পারে। ব্যবহারকারীরা, যারা ফিশিং আক্রমণ সম্পর্কে সচেতন নন, তারা ইমেলের সঙ্গে দেওয়া লিঙ্কটি ব্যবহার করে মিথ্যা ওয়েবসাইটে লগইন করতে পারেন, লোভনীয় অফার থেকে পণ্য নির্বাচন করতে পারেন এবং পিনসহ তার কার্ডের তথ্য সরবরাহ করতে পারেন। এই ধরনের সব তথ্য হ্যাকারের ডাটাবেসে ক্যাপচার করা হয়।

হ্যাকার এখন ইন্টারনেটে মূল্যবান জিনিসপত্র কেনার জন্য জালিয়াতির মাধ্যমে সংগৃহীত কার্ডের তথ্য ব্যবহার করতে পারে বা ক্যাপচার করা তথ্য ব্যবহার করে জাল কার্ড তৈরি করতে পারে বা এটিএম থেকে টাকা তুলতে পারে।

সব ব্যবসায়ীর সঠিক ওয়েবসাইট ঠিকানা জানা গ্রাহকদের পক্ষে সম্ভব নয়। মার্চেন্ট যে ব্যাংকের সঙ্গে লিঙ্ক করেছেন তার ঠিকানাও জানা সম্ভব নয়, কারণ মার্চেন্ট বিশ্বের যে কোনো ব্যাংকের সঙ্গে লিঙ্ক করা থাকতে পারে। অন্যদিকে গ্রাহক হয়তো অন্য কোনো ব্যাংকের কার্ড ব্যবহার করছেন।

তাই একটি ব্যাংকের ওয়েবসাইট, যা কার্ডের তথ্য সংগ্রহ করে সেটি একটি সার্টিফায়িং অথোরিটি যেমন VeriSign দ্বারা প্রত্যয়িত হতে পারে। যে ব্যাংক কার্ডের তথ্য সংগ্রহ করে তার পৃষ্ঠায় সার্টিফায়িং অথোরিটির সিলমোহর প্রদর্শিত হবে। যদি কোনো গ্রাহক সিলটিতে ক্লিক করেন তবে সার্টিফায়িং অথোরিটির ওয়েবসাইট প্রদর্শিত হবে। সব গ্রাহকের অবশ্যই প্রতিষ্ঠিত সার্টিফায়িং অথোরিটির ওয়েব ঠিকানা জানতে হবে এবং এভাবে এর সঠিকতা যাচাই করতে হবে। সার্টিফায়িং অথোরিটির ওয়েবসাইটের ঠিকানা সঠিক হলে, ব্যাংকের ওয়েবসাইটের পৃষ্ঠাও সঠিক। ফলে গ্রাহক এই ওয়েবপেজে নিরাপদে কার্ডের তথ্য সন্নিবেশ করতে পারেন।

**গ. প্রত্যাখ্যান (Repudiation) এবং ডিজিটাল স্বাক্ষর (Digital Signature)**

কখনও কখনও কিছু গ্রাহক ই-কমার্স বা ইন্টারনেট ব্যাংকিং সিস্টেমের মাধ্যমে ইন্টারনেটে কিছু কার্যকলাপ করে এবং অস্বীকার করে যে তিনি এটি করেননি, বরং ব্যাংক অফিসারদের দোষারোপ করেন যে তারা সিস্টেম থেকে তার পিন জানতে পারে এবং তা ব্যবহার করে অর্থ স্থানান্তর করার জন্য লেনদেন করতে পারে। এটি নিশ্চিত যে ব্যাংক অফিসারের পক্ষে গ্রাহকের পিনে অ্যাক্সেস নেই। কারণ সব পিন যুক্তিযুক্তভাবে এমন একটি সিস্টেমে রেকর্ড করা হয় যেখানে কোনো ব্যাংক অফিসার এমনকি প্রশাসকেরও অ্যাক্সেস নেই।

তাছাড়া সিস্টেমে ইলেকট্রনিক রেকর্ড রয়েছে—যা সহজেই চূড়ান্ত সুবিধাভোগীর নাম এবং ঠিকানাসহ লেনদেনের ইতিহাস তৈরি করতে পারে, যা থেকে প্রমাণিত হবে যে, ব্যাংক অফিসার কোনো সুবিধাভোগী নন। তবে এটি গ্রাহকদের বোঝানো খুব কঠিন হয়ে পড়ে। ডিজিটাল স্বাক্ষর এর একটি সমাধান।

ডিজিটাল স্বাক্ষর হলো প্রেরকের প্রাইভেট কী যা ব্যবহার করে ইলেকট্রনিকভাবে একটি বার্তা বা লেনদেন স্বাক্ষর করা (বা এনক্রিপ্ট করা) হয় এবং যা শুধু প্রেরকের পাবলিক কী ব্যবহার করে প্রাপকের দ্বারা পড়া (বা ডিক্রিপ্ট করা) যায়। পাবলিক এবং প্রাইভেট কী এর জোড়া একটি ইস্যুকারী কর্তৃপক্ষ (সাধারণত একটি সরকারি কর্তৃপক্ষ, বাংলাদেশে এটি বাংলাদেশ কম্পিউটার কাউন্সিল ও বাংলাদেশ ব্যাংক) দ্বারা একজন ব্যবহারকারীকে প্রদান করা হয়। তারপর ব্যবহারকারী তার পাবলিক কী অন্য ব্যবহারকারী বা প্রতিষ্ঠানের কাছে পাঠায় যাদের সঙ্গে সে ইলেকট্রনিক তথ্য বিনিময় করতে চায় (যেমন ইমেল বা ব্যাংকিং লেনদেন) এবং তার ব্যক্তিগত কী তার কাছে (তার কম্পিউটার বা পেনড্রাইভে) রাখে। এখন সে তার ব্যক্তিগত কী ব্যবহার করে সমস্ত সংবেদনশীল তথ্য এনক্রিপ্ট বা স্বাক্ষর করবে এবং অন্য পক্ষকে পাঠাবে। অন্যপক্ষ শুধু তার পাবলিক কী ব্যবহার করে ইমেইল খুলতে বা তথ্য ডিক্রিপ্ট করতে সক্ষম হবে। এটি নিশ্চিত করে যে লেনদেনটি ব্যবহারকারী নিজেই করেছেন। ব্যবহারকারী যদি এই ধরনের লেনদেন প্রত্যাখ্যান করেন, তাহলে আদালত আইসিটি আইন ২০০৬-এর ভিত্তিতে এই বিষয়ে ব্যাংকের পক্ষে রায় পাওয়া যেতে পারে।

ব্যাংক এমন একটি সিস্টেম তৈরি করতে পারে, যা শুধু গ্রাহকের কাছ থেকে তার ব্যক্তিগত কী ব্যবহার করে এনক্রিপ্ট করা লেনদেনের অনুরোধ পাবে। ই-কমার্স ব্যবহার করে লেনদেন করতে ইচ্ছুক সব গ্রাহককে ইস্যুকারী কর্তৃপক্ষের কাছ থেকে পাবলিক এবং প্রাইভেট কী সংগ্রহ করতে হয় এবং তার পাবলিক কী ব্যাংকে জমা দিতে হয়। পূর্বনির্ধারিত পরিমাণের ওপরে লেনদেনের জন্য (যেমন ৫০,০০০ টাকার উপরে লেনদেনের জন্য) এটি বাধ্যতামূলক করা যেতে পারে।

### ঘ টু-ফ্যাক্টর অথেটিকেশন (Two-Factor Authentication)

হ্যাকাররা গ্রাহকের কার্ডের পিন হ্যাক করে তা ই-কমার্স এবং ইন্টারনেট ব্যাংকিং সিস্টেমে অননুমোদিত লেনদেন করার জন্য ব্যবহার করতে পারে। এই ধরনের লেনদেন সুরক্ষিত করার জন্য, ব্যাংকগুলো টু-ফ্যাক্টর অথেনটিকেশন চালু করতে পারে, যার অর্থ হলো গ্রাহককে অবশ্যই দুইটি ফ্যাক্টর ব্যবহার করে লেনদেনটি সম্পন্ন করতে হবে—একটি হলো পিন এবং অন্যটি হলো টোকেন যাকে ক্রিপ্টোগ্রাফিক বা ইউএসবি বা হার্ডওয়্যার টোকেন বলা হয়।

একটি টোকেন হলো একটি ছোট হার্ডওয়্যার যা গ্রাহককে ব্যাংক থেকে প্রদান করা হয়। ডিভাইসের ও অথেনটিকেশন সার্ভারের টোকেন অ্যালগরিদম একই, ফলে সার্ভারে এবং টোকেন উভয়ই প্রতিটি নির্দিষ্ট সময়ের পরে (যেমন ১ মিনিট পরপর) একই নম্বর তৈরি করে। পিন ইনপুট দেওয়ার পরে, ব্যবহারকারীকে তার টোকেনে প্রদর্শিত তার টোকেন নম্বরটি প্রবেশ করতে বলা হয়। সে তার টোকেন থেকে নম্বরটি সংগ্রহ


*USB টোকেন*

করে এবং সিস্টেমে ইনপুট দেয়। ই-কমার্স সিস্টেম বা ইন্টারনেট ব্যাংকিং সিস্টেম এই টোকেন নম্বর এবং টোকেন আইডিটি অথেনটিকেশন সার্ভারে প্রেরণ করে, যা নম্বরটির সঠিকতা পরীক্ষা করে। নম্বরটি সঠিক হলে লেনদেন সফল, অন্যথায় প্রত্যাখ্যাত হবে।

যেহেতু টোকেনটি একটি ভৌত ডিভাইস এবং ব্যবহারকারীর অন্তর্গত এবং রেনডম নম্বর তৈরি করে, হ্যাকার এটি ক্যাপচার করতে পারে কিন্তু পরবর্তী মিনিটে

এটি অবৈধ হয়ে যাবে। এইভাবে টু-ফ্যাক্টর অথেনটিকেশন গ্রাহকদের জন্য আরও নিরাপত্তা প্রদান করে এবং টোকেনটি গ্রাহকের নিজস্ব হওয়ায় একটি গ্রাহকের পক্ষে লেনদেন অস্বীকার করা থেকে ব্যাংককে রক্ষা করে।

## ৯. এম-কমার্স এবং মোবাইল ফাইন্যান্সিয়াল সার্ভিসেস (এমএফএস)

### ৯.১. এম-কমার্স কী?

মোবাইল কমার্স যা এম-কমার্স বা mCommerce নামেও পরিচিত, একটি মোবাইল ডিভাইস, যেমন একটি মোবাইল ফোন, একটি ব্যক্তিগত ডিজিটাল সহকারী (পিডিএ), একটি স্মার্টফোন বা অন্যান্য উদীয়মান মোবাইল সরঞ্জাম যেমন ড্যাশটপ মোবাইল ডিভাইস ব্যবহার করে বাণিজ্য পরিচালনা করার উপায়। .

১৯৯০-এর দশক জুড়ে ইন্টারনেট এবং ইকমার্সের প্রবর্তন ব্যবসায়ীদের ব্যবসা করার উপায় এবং গ্রাহকদের ব্যবসার সঙ্গে যোগাযোগ করার উপায়কে নতুন

আকার দিয়েছে। ব্যবসাগুলো অনেকগুলো প্রক্রিয়া স্বয়ংক্রিয় করার সুযোগ পেয়েছে, যা আগে ম্যানুয়ালি পরিচালনা করা হতো যেমন, অর্ডার করা থেকে শুরু করে গ্রাহক পরিষেবা পর্যন্ত।

মোবাইল কমার্স, প্রায়শই এম-কমার্স হিসাবে উল্লেখ করা হয়, ই-কমার্সের (যেমন স্বয়ংক্রিয়, ইলেকট্রনিক প্রক্রিয়া) দ্বারা তৈরি অগ্রগতির ওপর ভিত্তি করে বাণিজ্য পরিচালনা করে এবং তা আরও ব্যক্তিগতকৃত উপায়ে বৃহত্তর দর্শকদের কাছে পৌঁছাতে সাহায্য করে।

কম্পিউটারের চেয়ে অনেক বেশি লোকের মোবাইল ফোনে অ্যাক্সেস রয়েছে এবং এর মানে হলো যে এম-কমার্সে শুধু বড় ব্যবসাই নয়, ছোট ব্যবসা এবং ভোক্তাদেরও ব্যাপকভাবে সংযুক্ত করার সুযোগ রয়েছে। এই অর্থে, মোবাইল ফোনের ডিজিটাল ডিভাইড-এর সঙ্গে সংযুক্ত হওয়ার সম্ভাবনা রয়েছে এবং সংস্থা এবং ব্যক্তিদের একে অপরের কাছে আগের চেয়ে আরও সহজে পৌঁছানোর সুযোগ করে দেয়।

## ৯.২. এম-কমার্সের ইতিহাস

মোবাইল কমার্সের জন্ম ১৯৯৭ সালে যখন ফিনল্যান্ডের হেলসিঙ্কি এলাকায় প্রথম দুটি মোবাইল-ফোন সক্ষম কোকা-কোলা ভেন্ডিং মেশিন ইনস্টল করা হয়েছিল। মেশিনগুলো এসএমএস টেক্সট বার্তার মাধ্যমে মূল্য গ্রহণ করতে পারত। প্রথম মোবাইল ফোনভিত্তিক ব্যাংকিং পরিষেবাটি ১৯৯৭ সালে ফিনল্যান্ডের মেরিটা ব্যাংক এসএমএস ব্যবহার করে চালু করেছিল।

১৯৯৮ সালে, মোবাইল ফোনে ডাউনলোড হিসাবে ডিজিটাল সামগ্রীর প্রথম বিক্রয় সম্ভব হয়েছিল যখন প্রথম বাণিজ্যিক ডাউনলোডযোগ্য রিংটোনগুলো ফিনল্যান্ডে রাডিওলিন্‌জা (বর্তমানে এলিজা ওজি-এর অংশ) দ্বারা চালু হয়েছিল।

মোবাইল বাণিজ্যের জন্য দুটি প্রধান জাতীয় বাণিজ্যিক প্ল্যাটফর্ম ১৯৯৯ সালে চালু হয়েছিল : ফিলিপাইনে স্মার্ট মানি http://smart.com.ph/money/), এবং জাপানে NTT DoCoMo-এর আই-মোড ইন্টারনেট পরিষেবা। আই-মোড একটি বিপ্লবী রাজস্ব ভাগাভাগি পরিকল্পনা বাস্তবায়ন করে, যেখানে এনটিটি ডুকুমু ব্যবহারকারীদের সামগ্রীর জন্য ৯ শতাংশ ফি রাখে এবং এর ৯১ শতাংশ সামগ্রীর মালিককে ফেরত দেয়।

২০০০ সালের প্রথম দিকে মোবাইল-বাণিজ্য-সম্পর্কিত পরিষেবাগুলো দ্রুত ছড়িয়ে পড়ে। নরওয়ে মোবাইলের মাধ্যমে পার্কিং এ পেমেন্ট চালু করে। অস্ট্রিয়া মোবাইল ডিভাইসের মাধ্যমে ট্রেনের টিকিট কাটা শুরু করে। জাপান এয়ারলাইন মোবাইলের মাধ্যমে টিকিট ক্রয়ের ব্যবস্থা করে।

মোবাইল কমার্সের জন্য নিবেদিত প্রথম সম্মেলন জুলাই ২০০১ সালে লন্ডনে অনুষ্ঠিত হয়েছিল।

মোবাইল কমার্স কভার করার প্রথম বইটি হলো টমি আহনেনের এম-প্রফিটস্ যাহা ২০০২ সালে প্রকাশিত হয়েছিল।

মোবাইল কমার্স নিয়ে আলোচনা করার জন্য প্রথম ইউনিভার্সিটির শর্ট কোর্সটি ২০০৩ সালে অক্সফোর্ড বিশ্ববিদ্যালয়ে অনুষ্ঠিত হয়েছিল, যেখানে টমি আহনেন এবং স্টিভ জন্স বক্তৃতা দিয়েছিলেন। ২০০৮ সাল পর্যন্ত, UCL কম্পিউটার সায়েন্স এবং পিটার বেন্টলি মোবাইল কমার্সের ওপর ডেডিকেটেড কোর্স পরিচালনা করে।

পিডিএ এবং সেলুলার ফোন এত জনপ্রিয় হয়ে উঠেছে যে অনেক ব্যবসায়ী তাদের গ্রাহকদের সঙ্গে যোগাযোগ করার জন্য আরও কার্যকর উপায় হিসাবে মোবাইল কমার্স ব্যবহার করতে শুরু করেছে।

সম্ভাব্য মোবাইল বাণিজ্য বাজারকে কাজে লাগানোর জন্য, মোবাইল ফোন নির্মাতারা যেমন আই-ফোন, স্যামসোন, নোকিয়া, ইরিকসন, মটরোলা ইত্যাদি 'এটি এবং টি' ওয়্যারলেস এবং স্প্রেন্ট-এর মতো মোবাইল ক্যারিয়ারের সঙ্গে ওয়াপ-সক্ষম স্মার্টফোন তৈরি করতে কাজ করছে। স্মার্টফোন ফ্যাক্স, ই-মেইল, এবং ফোন হিসাবে ব্যবহারের সক্ষমতা রাখে।

আইফোন চালু হওয়ার পর থেকে, মোবাইল কমার্স এসএমএস সিস্টেম থেকে দূরে সরে গিয়ে প্রকৃত অ্যাপ্লিকেশন নির্ভর হয়ে পড়েছে। এসএমএসের উল্লেখযোগ্য নিরাপত্তা দুর্বলতা এবং যানজটের সমস্যা রয়েছে, যদিও এটি ব্যাপকভাবে সহজলভ্য এবং অ্যাক্সেসযোগ্য। উপরন্তু, আধুনিক মোবাইল ডিভাইসের সক্ষমতা বৃদ্ধির সঙ্গে সঙ্গে তাহাতে আরও বেশি বেশি এপ্লিকেশন লোড করা সম্ভব হচ্ছে, ফলে এম-কমার্স আরও বিস্তার লাভ করছে।

## ৯.৩. মোবাইল ফিন্যান্সিয়াল সার্ভিসেস (এমএফএস)

### ৯.৩.১. মোবাইল ফিন্যান্সিয়াল সার্ভিসেস (এমএফএস) কি?

MFS হলো একটি ব্যাংকিং ব্যবস্থা, যা মূলত ব্যাংকবিহীন জনগোষ্ঠীর জন্য যা ব্যবহার করে একজন নিবন্ধিত মোবাইল ধারক একজন এজেন্টের কাছ থেকে টাকা জমা ও উত্তোলন করতে পারেন, তার MFS অ্যাকাউন্ট থেকে অন্য MFS অ্যাকাউন্টে অর্থ স্থানান্তর করতে পারেন, বিদেশ থেকে রেমিট্যান্স গ্রহণ করতে পারেন, কেনাকাটার বিল এবং ইউটিলিটি বিল পরিশোধ করতে পারেন, বিভিন্ন সরকারি ভাতা ও বেতন পেতে পারেন এবং যে কোনো মোবাইলের জন্য এয়ারটাইম টপআপ করতে পারেন।

এম-কমার্স মোবাইল ব্যাংকিং কার্যক্রমের একটি অংশ। শপিং ও ইউটিলিটি বিলের পেমেন্ট এবং এয়ারটাইম রিচার্জ এম-কমার্স কার্যক্রমকে বোঝায়।

### ৯.৩.২. MFS কার্যক্রম

এমএফএস প্রায় সমস্ত গুরুত্বপূর্ণ রিটেইল ব্যাংকিং কার্যক্রম যেমন অ্যাকাউন্ট খোলা, নগদ এবং স্থানান্তর ইত্যাদি পরিচালনা করতে সাহায্য করে। রিটেইল ব্যাংকিংয়ের অন্য দুই ধরনের লেনদেন যেমন ক্লিয়ারিং ও পেমেন্ট অর্ডার বা ডিডি ইস্যু করা MFS এর মাধ্যমে সম্ভব নয়। MFS এর কার্যাবলি নিচে প্রদত্ত হলো :

- গ্রাহক নিবন্ধন : ব্যাংক কর্মকর্তাদের দ্বারা এজেন্ট এবং ব্যবসায়ীদের নিবন্ধন এবং এজেন্টদের দ্বারা গ্রাহকদের নিবন্ধন। গ্রাহক মানে ভোক্তা, এজেন্ট এবং ব্যবসায়ী।
- নগদ : ক্যাশ পয়েন্ট (এজেন্ট), ব্যাংক শাখা এবং এটিএমের মাধ্যমে ক্যাশ-ইন/ক্যাশ-আউট।
- পি২পি (ব্যক্তি থেকে ব্যক্তি) : এক গ্রাহকের MFS অ্যাকাউন্ট থেকে অন্য গ্রাহকের MFS অ্যাকাউন্টে তহবিল স্থানান্তর (দেশীয় রেমিট্যান্স)। একই গ্রাহকের ব্যাংক অ্যাকাউন্ট এবং MFS অ্যাকাউন্টের মধ্যে তহবিল স্থানান্তরও সম্ভব।
- পি২বি (ব্যক্তি থেকে ব্যবসা) : ইউটিলিটি বিল পেমেন্ট, শিক্ষার ফি প্রদান, মোবাইল টপআপ, মার্চেন্ট পেমেন্ট, বাস/রেলওয়ে/এয়ারলাইন টিকিট এবং সিনেমার টিকিট কেনা।
- বি২পি (ব্যবসা থেকে ব্যক্তি) : কর্পোরেট সংস্থা / শিল্প / অফিস ইত্যাদি দ্বারা বেতন বিতরণ এবং বৈদেশিক এক্সচেঞ্জ হাউস দ্বারা MFS অ্যাকাউন্টে বিদেশি রেমিট্যান্স পাঠানো।
- পি২জি (ব্যক্তি থেকে সরকার) : আয়কর, সিটি কর্পোরেশন ট্যাক্স, ইত্যাদি প্রদান।
- জি২পি (সরকার থেকে ব্যক্তি) : প্রাথমিক শিক্ষকদের বেতন, বয়স্ক ভাতা এবং মুক্তিযোদ্ধা ভাতা, ইত্যাদি বিতরণ।

#### ৯.৩.২.১. এজেন্ট এবং মার্চেন্ট নিবন্ধন

তিনটি ভিন্ন বৈশিষ্ট্যসহ তিন ধরনের MFS অ্যাকাউন্ট রয়েছে। যদি একটি অ্যাকাউন্ট এজেন্ট হিসাবে নিবন্ধিত হয়, তাহলে তিনি তিনটি আইটেমসহ একটি মেনু পাবেন : গ্রাহক নিবন্ধন, ক্যাশ-ইন এবং ক্যাশ-আউট যদি একটি অ্যাকাউন্ট একজন মার্চেন্ট হিসাবে নিবন্ধিত হয়, সে শুধু একটি মেনু আইটেম পাবে: মার্চেন্ট পেমেন্ট। যদি একটি অ্যাকাউন্ট একজন গ্রাহক হিসাবে নিবন্ধিত হয় তবে তিনি তহবিল স্থানান্তর, ইউটিলিটি বিল পরিশোধ, শিক্ষা ফি এবং চার্জ প্রদান, এয়ারটাইম টপআপ এবং টিকিট ক্রয় (বাস/ট্রেন/এয়ারলাইন/সিনেমা ইত্যাদি) এর মতো বিভিন্ন আইটেম সহ একটি মেনু পাবেন। কিছু সাধারণ লেনদেন হলো ব্যালেন্স চেক, লেনদেন অনুসন্ধান এবং পিন পরিবর্তন যা সবার জন্য প্রযোজ্য।

শুধু মনোনীত ব্যাংক কর্মকর্তারা এজেন্ট এবং ব্যবসায়ীদের নিবন্ধন করতে পারেন। ব্যাংক তার এজেন্ট হিসেবে দেশের বিভিন্ন স্থানে ছোট দোকান, মোবাইল অপারেটরের খুচরা বিক্রেতা, এনজিও অফিস এবং পোস্ট অফিসকে মনোনীত ও নিবন্ধন করতে পারে। এই এজেন্টগুলোকে 'ক্যাশ পয়েন্ট'ও বলা হয়, কারণ গ্রাহকরা এই এজেন্টগুলোর মাধ্যমে ব্যাংকে টাকা জমা দিতে বা ব্যাংক থেকে টাকা তুলতে পারে। এজেন্ট একজন গ্রাহকের জন্য একটি অ্যাকাউন্ট খুলতে পারেন।

#### ৯.৩.২.২. গ্রাহক নিবন্ধন

একজন গ্রাহক একটি KYC (Know Your Customer) ফর্ম পূরণ করেন এবং ব্যাংকের যে কোনো নির্বাচিত এজেন্টে MFS পরিষেবার জন্য নিবন্ধন করেন।

গ্রাহক নিবন্ধন (KYC) ফর্মটি এজেন্টের কাছে হস্তান্তর করে। এজেন্ট তার মোবাইল ডিভাইস থেকে *<ব্যাংকের সংক্ষিপ্ত কোড>*# যেমন *১৬২১৬# এ ডায়াল করে মোবাইল ব্যাংকিং মেনুতে প্রবেশ করেন। এরপর এজেন্ট মেনু থেকে 'রেজিস্ট্রেশন' নির্বাচন করেন এবং ভোক্তার মোবাইল নম্বর টাইপ করে সেন্ড চাপেন। মোবাইল ব্যাংকিং সিস্টেম গ্রাহকের সেল নম্বর গ্রহণ করে। সিস্টেমটি তারপর IVR-এর মাধ্যমে গ্রাহকের মোবাইলে একটি ভয়েস কল জেনারেট করে এবং জানিয়ে দেয় যে তিনি একটি মোবাইল অ্যাকাউন্ট খুলতে চলেছেন এবং যদি তিনি সত্যিই চালিয়ে যেতে চান তবে তাকে একটি পিন প্রদান করার জন্য অনুরোধ করা হয়। গ্রাহক (যিনি এখন এজেন্টের সামনে আছেন) তার মোবাইল ডিভাইসে তার কাঙ্ক্ষিত পিন টাইপ করবেন। এভাবে, রেজিস্ট্রেশন প্রক্রিয়ার প্রথম ধাপ শেষ হয়। গ্রাহককে তার অ্যাকাউন্ট নম্বর জানিয়ে একটি এসএমএস পাঠানো হবে। মোবাইল

অ্যাকাউন্ট নম্বর হলো গ্রাহকের মোবাইল নম্বর এবং একটি চেক ডিজিটের সমন্বয়। যদি মোবাইল নম্বরটি ০১২৩৩৪৪৫৫৬৬ হয় এবং চেকের সংখ্যাটি ৮ গণনা করা হয়, তাহলে মোবাইল অ্যাকাউন্ট নম্বরটি হবে ০১২৩৩৪৪৫৫৬৬৮। তবে চেক ডিজিট ছাড়াও শুধু মোবাইল নম্বরটিও মোবাইল অ্যাকাউন্ট নম্বর হতে পারে।

একটি মোবাইল নম্বর সর্বজনীন এবং অনেকের কাছে পরিচিত হতে পারে। একটি চেক ডিজিট একটি অজানা ব্যক্তির দ্বারা অবাঞ্ছিত অর্থ প্রেরণ প্রতিরোধ করে। গ্রাহক যাদের সঙ্গে তিনি লেনদেন করতে চান শুধু তাদের সঙ্গে চেক ডিজিট শেয়ার করবেন। অন্যদিকে, চেক ডিজিট টাইপিং ভুল, তথা ভুল অ্যাকাউন্টে অর্থ জমা বা স্থানান্তর প্রতিরোধ করে।

রেজিস্ট্রেশনের ধাপ-১ শেষ হওয়ার পর, গ্রাহক তার MFS অ্যাকাউন্টে টাকা জমা দিতে পারেন, কিন্তু অ্যাকাউন্টটি সম্পূর্ণ অনুমোদিত না হলে তা থেকে টাকা তুলতে পারবেন না। এজেন্টরা তারপর ব্যাংকের কাছাকাছি মোবাইল ব্যাংকিং অফিসে নিবন্ধন ফর্ম পাঠায়।

রেজিস্ট্রেশনের ধাপ ২ হল ব্যাংকের কর্মকর্তা বা ৩য় পক্ষের এজেন্টদের দ্বারা ডেটা এন্ট্রি করা। ধাপ-৩ হলো গ্রাহকের রেজিস্ট্রেশন (KYC) ফর্মে উল্লিখিত তার ব্যক্তিগত তথ্য, ছবিসহ সিস্টেমে প্রবেশ করানো এবং সিস্টেমে মোবাইল অ্যাকাউন্টটি অনুমোদন করা। ফলে মোবাইল অ্যাকাউন্টটি সম্পূর্ণরূপে অনুমোদিত হয় এবং গ্রাহক তৎক্ষণাৎ একটি নিশ্চিতকরণ এসএমএস পান।

ইদানীং বাংলাদেশ ব্যাংক কর্তৃক e-KYC চালু করায় গ্রাহককে আর KYC ফর্ম পূরণ করতে হয় না। গ্রাহক নিজেই তার ছবি, তার NID এর উভয় পার্শ্বের ছবি উঠায়ে একটি অ্যাকাউন্ট খুলতে পারেন। সিস্টেম NID ডেটাবেস থেকে ছবি ও NID ভেরিফাই করে NID সার্ভার থেকে গ্রাহকের অন্যান্য তথ্য নিয়ে এসে অ্যাকাউন্টটি খুলে ফেলে।

### ৯.৩.২.৩. ক্যাশ-ইন (Cash-in)

ক্যাশ-ইন হলো গ্রাহকের MFS অ্যাকাউন্টে টাকা জমা দেওয়ার প্রক্রিয়া। প্রাপকের অ্যাকাউন্ট নম্বর জানা থাকলে যে কেউ MFS অ্যাকাউন্টে টাকা জমা করতে পারে। এজেন্ট জমাদানকারীকে একটি জমা স্লিপ প্রদান করবে। অ্যাকাউন্ট হোল্ডার তার MFS অ্যাকাউন্টে জমা করা সংক্রান্ত একটি তাৎক্ষণিক এসএমএস পাবেন।

প্রথমত, গ্রাহক এজেন্টের হাতে টাকা প্রদান করে। এজেন্ট মোবাইল ব্যাংকিং মেনুতে প্রবেশ করেন এবং মেনু থেকে 'ক্যাশ-ইন' নির্বাচন করে। তিনি গ্রাহকের MFS অ্যাকাউন্ট নম্বর, জমা দেওয়ার পরিমাণ এবং তার নিজের পিন টাইপ করেন এবং ব্যাংকের শর্টকোডে পাঠান। ব্যাংকের ডেটা সেন্টারের সিস্টেমটি এজেন্টের MFS অ্যাকাউন্ট থেকে গ্রাহকের MFS অ্যাকাউন্টে সমপরিমাণ অর্থ স্থানান্তর করবে। তাই এজেন্ট তখনই এই অপারেশনটি করতে পারে (অর্থাৎ গ্রাহকের কাছ থেকে নগদ গ্রহণ করতে পারে) যখন তার অ্যাকাউন্টে পর্যাপ্ত তহবিল থাকে। তিনি একটি ব্যাংক শাখা বা অন্য এজেন্ট থেকে তার MFS অ্যাকাউন্টে তহবিল পুনরায় পূরণ করতে পারেন। যদি তিনি ক্যাশ-আউট লেনদেন করেন তবে তার MFS অ্যাকাউন্টটিতে টাকা জমা হয়।

### ৯.৩.২.৪. ক্যাশ-আউট (Cash-out)

ক্যাশ-আউট হলো গ্রাহকদের MFS অ্যাকাউন্ট থেকে টাকা তোলার প্রক্রিয়া। শুধুমাত্র অ্যাকাউন্টধারীই তার অ্যাকাউন্ট থেকে টাকা তুলতে পারবেন। তাকে তার মোবাইল ফোন ডিভাইসসহ এজেন্টের সামনে উপস্থিত থাকতে হয়।

এজেন্ট মোবাইল ব্যাংকিং মেনুতে প্রবেশ করেন এবং তার মেনু থেকে 'ক্যাশ-আউট' নির্বাচন করে। তিনি গ্রাহকের MFS অ্যাকাউন্ট নম্বর এবং উত্তোলনের পরিমাণ টাইপ করেন এবং সেন্ড বোতাম টিপুন। ব্যাংকের ডেটা সেন্টারের সিস্টেমটি গ্রাহকের মোবাইল নম্বরে একটি ভয়েস কল শুরু করবে, যা জানিয়ে দেয় যে তিনি তার MFS অ্যাকাউন্ট থেকে ঐ পরিমাণ টাকা তুলতে চলেছেন। যদি তিনি চালিয়ে যেতে চান, তাহলে তাকে এখনই তার পিন প্রবেশ করাতে হবে। গ্রাহক মোবাইল ডিভাইসের কীপ্যাডে তার পিন টাইপ করেন। সিস্টেমটি পিন পরীক্ষা করে এবং সঠিক পাওয়া গেলে, এটি গ্রাহকের MFS অ্যাকাউন্ট থেকে এজেন্টের MFS অ্যাকাউন্টে সমপরিমাণ অর্থ স্থানান্তর করে। তাৎক্ষণিক এসএমএস উভয় পক্ষকে পাঠানো হবে। তারপর গ্রাহক এজেন্টের কাছ থেকে তার টাকা পান।

ক্যাশ আউট প্রক্রিয়াটি গ্রাহক নিজেও তার মোবাইল ফোন থেকে শুরু করতে পারেন। এক্ষেত্রে তিনি নিজেই এজেন্ট নম্বর, টাকার পরিমাণ ও পিন টাইপ করেন। এজেন্ট অনুমোদন করলে, গ্রাহকের MFS অ্যাকাউন্ট থেকে এজেন্টের MFS অ্যাকাউন্টে সমপরিমাণ অর্থ স্থানান্তর হবে।

### ৯.৩.২.৫. মার্চেন্ট পেমেন্ট (Merchant Payment)

গ্রাহক একজন মার্চেন্টের কাছ থেকে কিছু আইটেম কেনেন এবং তার MFS অ্যাকাউন্ট থেকে অর্থপ্রদান করতে চান। লেনদেনটি মার্চেন্ট তার নিবন্ধিত মোবাইল ডিভাইস থেকে শুরু করবে। তিনি মেনুটি শুরু করেন এবং মেনু বিকল্পগুলো থেকে 'মার্চেন্ট পেমেন্ট' নির্বাচন করেন। তিনি গ্রাহকের MFS অ্যাকাউন্ট নম্বর এবং অর্থপ্রদানের পরিমাণ টাইপ করে 'পাঠান' বোতাম টিপুন। ব্যাংকের ডেটা সেন্টারে থাকা সিস্টেমটি গ্রাহকের মোবাইল নম্বরে একটি ভয়েস

কল শুরু করবে এবং জানিয়ে দেবে যে তিনি এই MFS অ্যাকাউন্ট থেকে মার্চেন্টকে ঐ পরিমাণ টাকা দিতে চলেছেন। যদি তিনি চালিয়ে যেতে চান তবে তাকে তার পিন কোড প্রবেশ করাতে হবে। এখন গ্রাহক মোবাইল ডিভাইসের কীপ্যাডে তার পিন কোড টাইপ করেন এবং 'সেন্ড' বোতাম টিপুন। সিস্টেমটি পিন পরীক্ষা করে এবং সঠিক পাওয়া গেলে, এটি গ্রাহকের MFS অ্যাকাউন্ট থেকে মার্চেন্টের MFS অ্যাকাউন্টে সমপরিমাণ অর্থ স্থানান্তর করে। তাৎক্ষণিক এসএমএস উভয় পক্ষকে পাঠানো হবে। তারপর মার্চেন্ট গ্রাহকের কাছে পণ্য হস্তান্তর করবে।

মার্চেন্ট পেমেন্ট গ্রাহক নিজেই নিজের মোবাইল থেকে শুরু করতে পারেন। এক্ষেত্রে তিনি মার্চেন্টের নম্বর, বিলের পরিমাণ ও তার পিন টাইপ করেন। ফলে গ্রাহকের MFS অ্যাকাউন্ট থেকে এজেন্টের MFS একাউন্টে ঐ পরিমাণ টাকা স্থানান্তর হবে এবং মার্চেন্ট এসএমএসের মাধ্যমে তা জানতে পারবেন। তারপর মার্চেন্ট গ্রাহকের কাছে পণ্য হস্তান্তর করবেন। ইদানীং গ্রাহক মার্চেন্টের টেবিলে রক্ষিত QR Code স্ক্যান করেও মার্চেন্ট পেমেন্ট করতে পারবেন।

### ৯.৩.২.৬.ফান্ড ট্রান্সফার (Fund Transfer)

এই ক্রিয়াকলাপটি সেই গ্রাহক দ্বারা শুরু করা হয়, যিনি তার MFS অ্যাকাউন্ট থেকে অন্য MFS অ্যাকাউন্টে তহবিল স্থানান্তর করতে চান। গ্রাহক তার মোবাইল ডিভাইস থেকে *<ব্যাংকের সংক্ষিপ্ত কোড># যেমন *১৬২১৬# টাইপ করে মোবাইল ব্যাংকিং মেনুতে প্রবেশ করেন। গ্রাহক তারপরে তহবিল স্থানান্তর মেনু নির্বাচন করে, সুবিধাভোগীর MFS অ্যাকাউন্ট নম্বর, টাকার পরিমাণ এবং তার পিন কোড টাইপ করে। সিস্টেম এই কমান্ডটি গ্রহণ করবে এবং গ্রাহকদের MFS অ্যাকাউন্ট থেকে সুবিধাভোগীর MFS অ্যাকাউন্টে তহবিল স্থানান্তর করবে। তাৎক্ষণিক এসএমএস উভয় পক্ষকে পাঠানো হবে।

গ্রাহক যদি 'ব্যাংক অ্যাকাউন্টে/থেকে তহবিল স্থানান্তর' মেনু নির্বাচন করেন, তাহলে তিনি তার ব্যাংক অ্যাকাউন্ট এবং MFS অ্যাকাউন্টের মধ্যে তহবিল স্থানান্তর করতে সক্ষম হবেন। শর্ত: গ্রাহকের অবশ্যই একটি ব্যাংক অ্যাকাউন্ট থাকতে হবে এবং এই পরিষেবার জন্য প্রাক-নিবন্ধিত থাকতে হবে।

### ৯.৩.২.৭. গ্রাহকদের জন্য প্রাপ্ত অন্যান্য পরিষেবা

১. একজন গ্রাহক তার MFS অ্যাকাউন্ট থেকে ইউটিলিটি কোম্পানি/শিক্ষা প্রতিষ্ঠানের মোবাইল অ্যাকাউন্টে অর্থ স্থানান্তর করে ইউটিলিটি বিল (বিদ্যুৎ, গ্যাস, পানি, টেলিফোন ইত্যাদি) এবং শিক্ষা ফি পরিশোধ করতে পারেন।

২. একজন গ্রাহক তার MFS অ্যাকাউন্ট থেকে টাকা ট্রান্সফার করে বাস, ট্রেন, বিমান, সিনেমা এবং নাটকের টিকিট কিনতে পারেন।

৩. একজন গ্রাহক তার MFS অ্যাকাউন্ট থেকে মোবাইল অপারেটরের অ্যাকাউন্টে টাকা পরিশোধ করে এয়ারটাইম কিনতে পারেন।

৪. অফিস, কোম্পানি এবং শিল্প কোনো ব্যাংকের মোবাইল ব্যাংকিং প্ল্যাটফর্ম ব্যবহার করে তাদের কর্মচারীর বেতন তাদের ব্যক্তিগত MFS অ্যাকাউন্টে বিতরণ করতে পারে।

৫. সরকারি কর্তৃপক্ষ প্রাথমিক শিক্ষকদের বেতন, বয়স্ক ভাতা এবং মুক্তিযোদ্ধা ভাতা সুবিধাভোগীদের MFS অ্যাকাউন্টে বিতরণ করতে পারে।

৬. বাংলাদেশি প্রবাসীরা তাদের কাছের এবং প্রিয়জনের MFS অ্যাকাউন্টে টাকা পাঠাতে পারেন। প্রাপক (বেনিফিসিয়ারি) যে কোনো এজেন্ট, এটিএম বা শাখা থেকে টাকা তুলতে পারবেন। এটি রেমিট্যান্সের লাস্ট মাইল ডেলিভারিকে আরও প্রশস্ত করেছে।

### ৯.৩.৩. পিন কে দেবে?

যে অ্যাকাউন্টধারীর অ্যাকাউন্টটি ডেবিট করা হবে তিনি লেনদেনের অনুমোদনের জন্য তার পিন প্রদান করবেন।

### ৯.৩.৪. এমএফএস-এ লেনদেনের সীমা

এমএফএস বিপুল পরিমাণ অর্থ লেনদেনের জন্য ব্যবহার করা হয় না। ব্যাংক এজেন্টের মাধ্যমে টাকা জমা এবং উত্তোলনের জন্য একটি সীমা নির্ধারণ করে। ব্যাংকটি এক দিনে এবং এক মাসে সর্বাধিক সংখ্যক লেনদেনও নির্ধারণ করে। উদাহরণস্বরূপ, একজন গ্রাহককে একবারে সর্বোচ্চ ৫,০০০/- টাকা তোলা বা জমা দেওয়ার অনুমতি দেওয়া যেতে পারে এবং দিনে ৫টি এই ধরনের লেনদেন করা যেতে পারে, তবে মাসে ২০টির বেশি লেনদেন করা যাবে না। এই ধরনের সীমা নির্ধারণের মাধ্যমে ব্যাংক মোবাইল ব্যাংকিংয়ের মাধ্যমে প্রতারনার ঝুঁকি কমাতে পারে। যেহেতু মোবাইল প্ল্যাটফর্ম ব্যবহার করে যোগাযোগ ১০০% নিরাপদ নয়, তাই ব্যাংকগুলো মোবাইল চ্যানেলগুলো ব্যবহার করে প্রচুর পরিমাণে এবং বৃহৎ সংখ্যক লেনদেনের অনুমতি দেয় না।

এজেন্টদের জন্যও সীমা নির্ধারণ করা যেতে পারে যেমন তিনি একদিনে ২০০টির বেশি ক্যাশ-ইন/আউট লেনদেন করতে পারবেন না এবং মাসে ৪০০০টির বেশি লেনদেন করতে পারবেন না। মার্চেন্টের জন্যও লেনদেনের সীমা নির্ধারণ করা যায়। গ্রাহকদের অন্যান্য সীমার মধ্যে P2P ফান্ড ট্রান্সফার, মার্চেন্ট পেমেন্ট, ইউটিলিটি বিল পেমেন্ট, এয়ারটাইম টপ আপ, টিকিট কেনা, ব্যাংক অ্যাকাউন্ট এবং MFS অ্যাকাউন্টের মধ্যে ফান্ড ট্রান্সফারের মতো বিভিন্ন পরিষেবার জন্য

লেনদেনের পরিমাণ এবং সংখ্যার সীমাবদ্ধতা (একদিন এবং মাসে) অন্তর্ভুক্ত থাকতে পারে।

### ৯.৩.৫. এমএফএস কি ব্যয়বহুল?

গ্রাহকরা তাদের MFS অ্যাকাউন্টে তাদের জমার ওপর সুদ পান না। অন্যদিকে, গ্রাহককে তার মোবাইল অ্যাকাউন্টে লেনদেনের জন্য এজেন্ট বা ব্যাংককে ফি দিতে হয়। ফলে MFS গ্রাহকদের জন্য সস্তা নয়।

এমএফএস সেটআপ এবং রক্ষণাবেক্ষণ ব্যাংকগুলোর জন্য ব্যয়বহুল। প্রয়োজনীয় সফ্টওয়্যার এবং হার্ডওয়্যারগুলোর উচ্চ ব্যয়ের কারণে প্রাথমিক ব্যয়টি খুব বেশি। সারা দেশে এজেন্টদের একটি বৃহৎ গ্রুপ পরিচালনা করা খুব ব্যয়বহুল। দেশব্যাপী কেওয়াইসি যাচাইয়ের জন্য ব্যাংককে বিপুলসংখ্যক কর্মচারীকে জড়িত করতে হবে।

### ৯.৩.৬. এমএফএসে মডেল : ব্যাংক-লেড ও টেলকো-লেড (Bank-Led and Telco-Led)

এমএফএসের দুটি মডেল রয়েছে : ব্যাংক-লেড এবং টেলকো-লেড। ব্যাংক-লেড মডেলটিতে, ব্যাংক তার গ্রাহকদের কেওয়াইসির (Know Your Customer) জন্য দায়বদ্ধ এবং প্রতিটি গ্রাহকের অর্থ এবং তথ্যের রক্ষক। এটি সত্য প্রতিষ্ঠিত যে ব্যাংকগুলো গ্রাহকের যথাযথ কেওয়াইসি নিশ্চিত করতে অভিজ্ঞ। কেন্দ্রীয় ব্যাংকের এবং অভ্যন্তরীণ নিরীক্ষকরা পর্যায়ক্রমে কেওয়াইসির সঠিকতা পরীক্ষা করা প্রয়োজন।

কয়েকশ বছর ধরে, ব্যাংকগুলো আমানতের রক্ষক হিসাবে খুব বেশি বিশ্বস্ত। কেন্দ্রীয় ব্যাংকের অনেকগুলো প্রক্রিয়া এবং নিয়ন্ত্রণ রয়েছে, যার মাধ্যমে তা নিশ্চিত করা হয়। এবং গ্রাহক চাহিবা মাত্রই ব্যাংক গ্রাহকের অর্থ ফেরত দিতে বাধ্য। এই জাতীয় প্রক্রিয়াগুলোর মধ্যে রয়েছে যথাযথ তরলতা, সিএআর (মূলধন পর্যাপ্ততার অনুপাত), সিআরআর (নগদ রিজার্ভের প্রয়োজনীয়তা) এবং এসএলআর (বিধিবদ্ধ তরলতার অনুপাত) বজায় রাখা। কেন্দ্রীয় ব্যাংকের এই প্রয়োজনীয়তাগুলো কোনো একটি ব্যাংকের স্বাস্থ্যকে ভালো রাখতে এবং আমানতকারীর আমানত রক্ষা করতে সাহায্য করে।

গ্রাহকের তথ্য, লেনদেনের প্রকৃতি এবং অ্যাকাউন্টে ভারসাম্যের গোপনীয়তা বজায় রাখা ব্যাংকের একটি বাধ্যতামূলক করণীয়। এই কারণেই ব্যাংক তার গ্রাহকের ডাটাবেসকে শেয়ারড্ সফ্টওয়্যার বা তৃতীয় পক্ষের দ্বারা রক্ষণাবেক্ষণ করা কোনো সফটওয়্যার সিস্টেমে রাখতে পারে না। সমস্ত পশ্চিমা দেশ এবং আমাদের প্রতিবেশী ভারত এবং পাকিস্তান MFS-এর জন্য এক ধরনের ব্যাংক লেড মডেল অনুসরণ করে।

অন্যদিকে, টেলকো-লেড মডেলটিতে, মোবাইল সংস্থা গ্রাহকের কেওয়াইসি এবং আমানতকারীর অর্থ এবং তথ্যের জন্য দায়বদ্ধ। তবে তাদের এক বা একাধিক ব্যাংকে তাদের MFS-এ জমাকৃত অর্থের সমতুল্য টাকা জমা রাখতে হয়। কেনিয়া, ফিলিপাইন এবং অন্যান্য অনুরূপ কিছু দেশ টেলকো-লেড মডেল চালু করেছে।

ব্যাংক-লেড মডেলটিতে, গ্রাহকের আমানত এবং তথ্য রক্ষার জন্য, ব্যাংক নিম্নলিখিতগুলো নিশ্চিত করবে :

ক. মোবাইল অ্যাকাউন্টটি সক্রিয় হওয়ার আগেই গ্রাহকদের কেওয়াইসি ব্যাংক নিজস্ব ব্যবস্থাপনায় যাচাই করে নেবে, যাতে কোনো কর্তৃপক্ষ ব্যাংককে তার কোনো গ্রাহককে শনাক্ত করতে বলে, ব্যাংক সেই গ্রাহককে যথাযথভাবে শনাক্ত করতে পারে।

খ. সফ্টওয়্যার এবং হার্ডওয়্যার সিস্টেমটি ব্যাংক নিজেই সংরক্ষণ ও রক্ষণাবেক্ষণ করবে যাতে, যদি কোনো কর্তৃপক্ষ ব্যাংককে নির্দিষ্ট মোবাইল অ্যাকাউন্টে লেনদেন বন্ধ করতে বলে, ব্যাংক অন্য পক্ষের ওপর কোনো নির্ভরতা ছাড়াই এটি করতে পারে এবং যখন কর্তৃপক্ষ ব্যাংককে একটি নির্দিষ্ট মোবাইল অ্যাকাউন্টের লেনদেনের ইতিহাস জমা দিতে বলুন, ব্যাংকটি তাৎক্ষণিকভাবে সেটি জমা দিতে পারে। গ্রাহকের ডেটা সুরক্ষা এবং গ্রাহকের অ্যাকাউন্টের গোপনীয়তা এবং সুরক্ষার জন্য এটি প্রয়োজন।

গ. ব্যাংকের সমস্ত MFS অ্যাকাউন্টের মোট আমানত পরিমাণ ব্যাংকের ব্যালেন্স শিটে দেখানো উচিত এবং এইভাবে প্রয়োজনীয় সিআরআর (নগদ রিজার্ভের অনুপাত) এবং এসএলআর (বিধিবদ্ধ তরলতার অনুপাত) কেন্দ্রীয় ব্যাংকের সঙ্গে বজায় রাখা উচিত, প্রয়োজনীয় মূলধন, CAR (মূলধন পর্যাপ্ততার অনুপাত) এবং কেন্দ্রীয় ব্যাংকের গাইডলাইন অনুসারে এই জাতীয় অন্যান্য সুরক্ষা গ্রহণ করতে পারে। তবে, ২০২১ সালে বাংলাদেশের কেন্দ্রীয় ব্যাংক 'ব্যাংক-লেড মডেল'-কে 'ব্যাংক-NBFI-সরকার-নেতৃত্বাধীন মডেল' দ্বারা প্রতিস্থাপন করেছে। এর অর্থ, কোনো ব্যাংক বা অ-ব্যাংকিং আর্থিক প্রতিষ্ঠান বা সরকারি সংস্থা/বিভাগের কমপক্ষে ৫১% ভাগ এবং বাকি অংশ যে কোনো সংস্থা গ্রহণ করে বাংলাদেশে এমএফএস গঠন করা যেতে পারে।

### ৯.৩.৭. সংযোগ—এসএমএস (SMS) বনাম ইউএসএসডি (USSD)

এজেন্ট/মার্চেন্ট/গ্রাহক, এসএমএস (শর্ট মেসেজিং সিস্টেম) বা ইউএসএসডি (আনস্ট্রাকচার্ড সাপ্লিমেন্টারি সার্ভিস ডেটা) ব্যবহার করে ব্যাংকের মোবাইল ব্যাংকিং সিস্টেম এবং তাদের মোবাইল ডিভাইসের মধ্যে সংযোগ স্থাপন করতে পারে। এসএমএস সংযোগ সুরক্ষিত মিডিয়া নয়, তবে ইউএসএসডি অপেক্ষাকৃত সুরক্ষিত। এসএমএস এবং ইউএসএসডি চ্যানেলগুলোর মধ্যে একটি তুলনা নিচে দেওয়া হয়েছে—

| আইটেম | এসএমএস (SMS) | ইউএসএসডি (USSD) |
|---|---|---|
| ডেটা ফর্ম্যাট | এসএমএস বার্তাগুলোর জন্য ব্যবহৃত ডেটা ফর্ম্যাটটি হলো টেক্সট। | ডিফল্ট ডেটা ফর্ম্যাটটি আনস্ট্রাকচারযুক্ত। (Unstructured) |
| এনক্রিপশন | ক্লায়েন্ট এবং ব্যাংক সার্ভারের মধ্যে অ্যান্ড-টু-অ্যান্ড এনক্রিপশন নেই। | ক্লায়েন্ট এবং ব্যাংক সার্ভারের মধ্যে অ্যান্ড-টু-এ্যান্ড এনক্রিপশন তৈরি করা হয়। |
| ডেটা স্টোরেজ | এসএমএস এ ডেটা প্রথমে স্টোর করা হয়, তারপর প্রেরন করা হয়। | ইউএসএসডি কোথাও ডেটা স্টোর করে না। |
| সেশন বা মেয়াদ | এসএমএস ব্যাংকিং সেশনভিত্তিক। | যখন কোনো ব্যবহারকারী ইউএসএসডি পরিষেবা অ্যাক্সেস করে, তখন একটি অধিবেশন প্রতিষ্ঠিত হয়, এবং গ্রাহক অ্যাপ্লিকেশনটি বন্ধ না করা পর্যন্ত সংযুক্ত থাকে। |

## ১০. এজেন্ট ব্যাংকিং

এজেন্ট ব্যাংকিং সিস্টেম, আউটসোর্সড এজেন্টদের মাধ্যমে সমাজের নিম্নবিত্ত/সুবিধাবঞ্চিত জনগোষ্ঠীর দোরগোড়ায় ব্যাংকিং সেবা পৌঁছে দেয়। আউটসোর্সড এজেন্ট গ্রামীণ অঞ্চলের এমন এলাকায় এজেন্ট ব্যাংকিং আউটলেট খোলে যেখানে কোনো ব্যাংকের শাখা নেই। এজেন্ট আউটলেটটি একটি ব্যাংকের পক্ষে গ্রাহকদিগকে ব্যাংকিং পরিষেবা প্রদান করে এবং ব্যাংকিং সেবা বঞ্চিত জনগণের মধ্যে দূরত্ব লাগব করে। এই পদ্ধতিতে লেনদেন প্রক্রিয়াটি সহজতর করার পাশাপাশি বায়োমেট্রিক অথেনটিকেশনের মাধ্যমে সুরক্ষিত করা হয় এবং তা রিয়েল টাইম ভিত্তিতে সম্পন্ন হয় এবং গ্রাহকরা তাদের বাড়ির কাছে ব্যাংকিং সেবা পেয়ে থাকেন।

এজেন্ট ব্যাংকিংয়ের উদ্দেশ্য হলো ব্যাংকিং পরিষেবাগুলো ঐ জাগায় পৌঁছাতে যেখানে ব্যাংক শাখাগুলোর সম্প্রসারণ আর্থিকভাবে লাভজনক নয়। এজেন্ট ব্যাংকিং ব্যাংকের জন্য একটি কার্যকর বিকল্প।

### ১০.১ এজেন্ট ব্যাংকিংয়ের ইতিহাস

এজেন্ট ব্যাংকিংয়ের ধারণাটি ব্রাজিল, কলম্বিয়া এবং পেরুর মতো দক্ষিণ আমেরিকার বেশ কয়েকটি উন্নয়নশীল দেশ থেকে এসেছে। দেশগুলোর মধ্যে ব্রাজিল এজেন্ট ব্যাংকিংয়ের অগ্রগামী হিসাবে স্বীকৃত। এজেন্ট ব্যাংকিং প্রথম বাংলাদেশে বাংলাদেশ ব্যাংক (সেন্ট্রাল ব্যাংক অব বাংলাদেশ) দ্বারা ২০১৩ সালে প্রবর্তিত হয়েছিল। এরই ধারাবাহিকতায়, বাংলাদেশ ব্যাংক ২০১৭ সালে বাংলাদেশে এজেন্ট ব্যাংকিং অপারেশনের জন্য একটি বিস্তৃত গাইডলাইন জারি করে, যাতে এজেন্টের অনুমোদনের প্রক্রিয়া, প্রযোজ্য কার্যাবলি, ব্যাংক এবং এজেন্টদের দায়িত্ব, এএমএল/সিএফটি-এর প্রয়োগ, গ্রাহক সুরক্ষা এবং ব্যবসায়িক ধারাবাহিকতা বজায় রাখার কৌশল ইত্যাদি বর্ণিত হয়। এই গাইডলাইন দেশে এজেন্ট ব্যাংকিংয়ের নিরাপদ ও কার্যকর প্রসারণে এবং বাংলাদেশে আর্থিক অন্তর্ভুক্তিতে অনুঘটক হিসাবে কাজ করেছে। পরে ভারত, মালয়েশিয়া, কেনিয়া, পাকিস্তান এবং ফিলিপিন্সের মতো অন্যান্য দেশে ধীরে ধীরে এজেন্ট ব্যাংকিংয়ের কার্যক্রম শুরু হয়।

### ১০.২ এজেন্ট ব্যাংকিং চালু করার পেছনে কৌশল

এজেন্ট ব্যাংকিং প্রবর্তনের পেছনে সামগ্রিক কৌশল হলো সুবিধাবঞ্চিত জনগোষ্ঠী, যারা ব্যাংকিং নেটওয়ার্কের নাগালের বাইরে প্রত্যন্ত অঞ্চলে বসবাস করেন, তাদের জন্য একটি নিরাপদ ব্যাংকিং ব্যবস্থা চালু করা। গ্রাহকদের আকৃষ্ট করা ও ধরে রাখা, আর্থিক সেবার উন্নতি এবং বিভিন্ন ধরনের পরিষেবা তৈরি করে মার্কেট শেয়ার বৃদ্ধি করাই হলো এজেন্ট ব্যাংকিংয়ের উদ্দেশ্য। প্রাথমিকভাবে, এজেন্ট ব্যাংকিং আমানত সংগ্রহের মধ্যে সীমাবদ্ধ ছিল, কিন্তু বর্তমানে এজেন্ট ব্যাংকিং গ্রামীণ অর্থনীতিকে শক্তিশালী করা এবং সুবিধাবঞ্চিত ব্যক্তিদের মধ্যে ঋণ প্রদান সহ সকল প্রকার ব্যাংকিং পরিষেবা প্রদানের মাধ্যমে ডিজিটাল বাংলাদেশ বিনির্মাণে গুরুত্বপূর্ণ ভূমিকা পালন করছে।

দেশের অর্থনৈতিক উন্নয়ন গ্রামীণ উন্নয়নের ওপর নির্ভর করে। ২০২১ সালের সেপ্টেম্বর পর্যন্ত বাংলাদেশে ৬১টি তফসিলি এবং ৫টি নন-তফসিলি ব্যাংক ছিল। বাজারের আকারের তুলনায় বাংলাদেশে ব্যাংকের সংখ্যা অনেক বেশি, তবে তৃণমূল পর্যায়ে ব্যাংকিং সেবার বিস্তৃতি ছিল খুবই নগণ্য। বাংলাদেশ ব্যাংক একটি প্রবিধান নিয়ে এসেছে যে, কোনো বেসরকারি ব্যাংক যদি শহরাঞ্চলে একটি শাখা খুলতে চায়, তবে তাদের গ্রামাঞ্চলে অন্তত একটি শাখা খুলতে হবে। নতুন শাখার উচ্চ ওভারহেড খরচ, রক্ষণাবেক্ষণ এবং কার্য পরিচালনামূলক খরচ এত বেশি যে, তা ব্যাংকগুলোকে নতুন শাখা খুলতে অনিচ্ছুক করে তোলে। এ কারণে জেলা পর্যায়েও অনেক ব্যাংকের শাখা নেই।

ফলস্বরূপ, গ্রামীণ এলাকার জনসংখ্যার একটি বড় অংশ ব্যাংকের নাগালের বাইরে, ফলে তারা আর্থিক অন্তর্ভুক্তির বাইরে থেকে যায়। তারা সাধারণত এনজিও, গ্রামীণ ব্যাংক এবং অন্যান্য নন-ব্যাংক আর্থিক প্রতিষ্ঠানের কাছে তাদের সঞ্চয় রাখে। ব্যাংকগুলো মূলত বিভিন্ন স্টেকহোল্ডারদের স্বার্থকে সামনে রেখে সেই নির্দিষ্ট বাজারকে লক্ষ্য করে এজেন্ট ব্যাংকিং চালু করে। এজেন্ট ব্যাংকিংয়ের মাধ্যমে দেশের গ্রামীণ জনগণ স্বল্পতম সময়ের মধ্যে সারা দেশে নগদ আদান-প্রদানের সুবিধা পাচ্ছে। ব্যাংকের সঙ্গে মানুষের সম্পৃক্ততা বেড়েছে, লেনদেন বেড়েছে, স্বল্পমূল্যে বিপুল আমানত সংগ্রহ হয়েছে, গ্রামীণ জনগণ ঋণ সুবিধা পাচ্ছে এবং মানুষের জীবনযাত্রার মান বৃদ্ধি পেয়েছে।

যদিও এজেন্ট ব্যাংকিং ব্যাংকিং-বঞ্চিত জনগনকে ব্যাংকিং ছাতার নিচে নিয়ে এসেছে, ব্যাংকগুলোর পরিকল্পনা হলো, দেশের প্রত্যন্ত ও প্রান্তিক অঞ্চলে এই সুবিধা ছড়িয়ে দেওয়া, যাতে প্রতিটি মানুষ সত্যিকারের ব্যাংকিং সুবিধা পায় এবং দেশের অর্থনৈতিক উন্নয়নে অংশ নিতে পারে। এজেন্ট ব্যাংকিং গ্রামীণ জনগণের জন্য একটি বিকল্প অথচ আকর্ষণীয় আর্থিক পরিষেবার মাধ্যম হয়ে ওঠার সম্ভাবনা রয়েছে।

### ১০.৩. বাংলাদেশে এজেন্ট ব্যাংকিংয়ের বর্তমান পরিস্থিতি

প্রতিষ্ঠার মাত্র দেড় বছরের মধ্যে, এজেন্ট ব্যাংকিং বিপুলসংখ্যক গ্রাহককে আকৃষ্ট করতে সক্ষম হয়েছে, যা অধিকাংশ বাণিজ্যিক ব্যাংককে শাখাভিত্তিক ব্যাংকিং ছাড়াও এই বিকল্প আর্থিক পরিষেবা চালু করতে বাধ্য করেছে।

যদিও কেন্দ্রীয় ব্যাংক ২০১৩ সালে একটি এজেন্ট ব্যাংকিং নির্দেশিকা জারি করেছিল, এজেন্ট ব্যাংকিংয়ের সম্পূর্ণ ক্রিয়াকলাপ ২০১৬ সালে শুরু হয়েছিল। সেই বছরের অক্টোবর থেকে ডিসেম্বরের মধ্যে ৫৪৪,৫৩৬টি অ্যাকাউন্ট এবং ৩৮০৬.৮ মিলিয়ন টাকা ডিপোজিটের মধ্য দিয়ে এজেন্ট ব্যাংকিং সফলভাবে শুরু হয়েছিল।

বাংলাদেশ ব্যাংকের জুন ২০২২-এর ত্রৈমাসিক প্রতিবেদন অনুসারে, বাংলাদেশে ৩০টি বাণিজ্যিক ব্যাংক ১৪,২৯৯টি এজেন্টের অধীনে ১৯,৭৩৭টি আউটলেটের মাধ্যমে এজেন্ট ব্যাংকিং কার্যক্রম পরিচালনা করেছে। আর বর্তমানে এজেন্ট ব্যাংকিং অ্যাকাউন্টের মোট সংখ্যা দাঁড়িয়েছে ১৬,০৭৪,৩৭৮, যেখানে ডিপোজিট রয়েছে ২৮০,৮৫৩.১৮ মিলিয়ন টাকা।

ব্যাংক এবং ক্লায়েন্ট উভয়ের জন্যই বিপুল সুবিধা থাকায় এজেন্ট ব্যাংকিং জনপ্রিয় হয়ে উঠেছে। এজেন্ট ব্যাংকিং এ ধরনের জনপ্রিয়তা অর্জন করতে সক্ষম হয়েছে মূলত গ্রাহকদের কাছে এর সরলতা এবং ব্যাংকের জন্য কম খরচে সেবা প্রদান সম্ভব হচ্ছে বলে। এজেন্ট ব্যাংকিংয়ের মাধ্যমে ব্যাংকগুলো গ্রাহকের সংখ্যা বাড়াতে, আর্থিক সেবার উন্নত করতে, অপারেটিং খরচ কমাতে, ব্যবসার সম্প্রসারণ করতে, আমানত সংগ্রহ বাড়াতে, ব্যাংকগুলোর ব্র্যান্ডিং উন্নত করতে এবং ব্যাংকের পরিসরকে প্রসারিত করতে সক্ষম হয়েছে।

এজেন্ট ব্যাংকিং প্রত্যন্ত অঞ্চলের গ্রাহকদের দোরগোড়ায় পূর্ণাঙ্গ ব্যাংকিং পরিষেবা পৌঁছানো সহজতর করেছে এবং এটি রেমিট্যান্স চ্যানেলকে সুবিধাজনক এবং সহজ করে তুলেছে।

৩০ জুন, ২০২২ পর্যন্ত, সারা দেশে ১৯,৭৩৭টি এজেন্ট ব্যাংকিং আউটলেটের মাধ্যমে ৯৭০,৪৮১.৮২ মিলিয়ন টাকার অভ্যন্তরীণ ফরেন রেমিটেন্স পাঠানো হয়েছে।

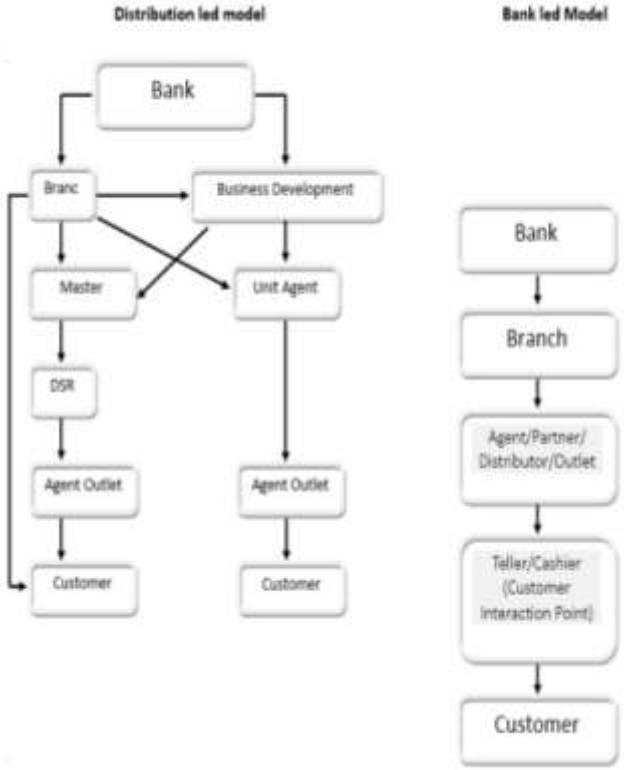
এজেন্ট ব্যাংকিং আউটলেটগুলো এখন কেবল নগদ জমা এবং নগদ উত্তোলন ও রেমিট্যান্স পেমেন্টের মতো পরিষেবাগুলোর মধ্যে সীমাবদ্ধ নয়, ব্যাংকগুলো আউটলেটগুলোর মাধ্যমে ছোট ঋণ দেওয়া শুরু করেছে এবং ২০২২ সালের ৩০ জুন পর্যন্ত, ৭৬,৪৫৬.৩৩ মিলিয়ন টাকা ঋণ বিতরণ করেছে।

### ১০.৪ বাংলাদেশে এজেন্ট ব্যাংকিং মডেল

মূলত, বাংলাদেশে সেবা প্রদানের জন্য ব্যাংকগুলো দুই ধরনের এজেন্ট ব্যাংকিং মডেল বজায় রাখছে। একটি হলো ডিস্ট্রিবিউশন লেড মডেল এবং অন্যটি হলো ব্যাংক লেড মডেল।

ডিস্ট্রিবিউশন-লেড মডেলে, অর্থ ব্যাংক থেকে ডিস্ট্রিবিউটর, ডিস্ট্রিবিউটর (এজেন্ট) থেকে আউটলেট এবং আউটলেট থেকে গ্রাহকের কাছে প্রবাহিত হয় এবং এর বিপরীতে গ্রাহকের কাছ থেকে ব্যাংকে অর্থ প্রবাহিত হয়। এই মডেলে, সারা দেশে বেশ কয়েকটি ব্যবসায়িক উন্নয়ন কেন্দ্র রয়েছে যেখানে এজেন্ট এবং সাব-এজেন্টদের তত্ত্বাবধান ও নিরীক্ষা করা এবং বাজারের উন্নয়নের জন্য ব্যাংকের কর্মকর্তারা নিয়োগপ্রাপ্ত হন। এই মডেলে, এজেন্ট একটি পরিবেশক হিসাবে কাজ করে এবং এর প্রধান দায়িত্ব হলো সাব-এজেন্ট/আউটলেটগুলোকে পুনঃভারসাম্য

করা (নগদের ঘাটতি হলে তা সরবরাহ করা বা অতিরিক্ত হলে তা নগদ সংগ্রহ করা)। এভাবে আউটলেটগুলোকে পুনঃভারসাম্যের জন্য ব্যাংক শাখায় যেতে হবে না। কিন্তু এই সার্ভিস প্রদানের বিপরীতে সাব-এজেন্টদের তাদের আয়ের একটি অংশ এজেন্টদের সঙ্গে ভাগ করে নিতে হবে।




ইউনিট এজেন্ট মডেলে, ইউনিট এজেন্ট হলো একটি আউটলেট যাহা এজেন্টের অধীনে ব্যবসা চালায় না, কিন্তু সরাসরি বিজনেস ডেভেলপমেন্ট অফিসে রিপোর্ট করে। এক্ষেত্রে টাকা ব্যাংক থেকে আউটলেট (ইউনিট এজেন্ট) আউটলেট থেকে গ্রাহকের কাছে প্রবাহিত হয় এবং এর বিপরীতে গ্রাহকের কাছ থেকে ব্যাংকে অর্থ প্রবাহিত হয়।

বিপরীতে ব্যাংক-লেড মডেলটি ইউনিট এজেন্ট মডেলের প্রায় অনুরূপ, যেখানে অর্থ ব্যাংক থেকে আউটলেটে, আউটলেট থেকে গ্রাহকের কাছে প্রবাহিত হয় এবং এর বিপরীতে গ্রাহকের কাছ থেকে ব্যাংকে অর্থ প্রবাহিত হয়। মডেলটিতে, কোনো ব্যবসায়িক উন্নয়ন কেন্দ্র নেই, তবে ব্যাংকের দু-একজন নিজস্ব কর্মকর্তা আউটলেটে বসে সরাসরি এজেন্ট আউটলেটটি পর্যবেক্ষণ করেন ও সহায়তা প্রদান করেন। যদি একটি নির্দিষ্ট ব্যাংকের শাখা এজেন্ট আউটলেট থেকে অনেক দূরে থাকে, তাহলে নগদ ভারসাম্য বজায় রাখা খুব কঠিন হয়ে পড়ে (হয় নগদের ঘাটতি জোগান দেওয়া বা অতিরিক্ত নগদ সংগ্রহ করা কঠিন হয়ে পড়ে)।

### ১০.৫. এজেন্ট ব্যাংকিংয়ের সঙ্গে জড়িত পক্ষগুলো

**এজেন্ট :** এজেন্ট বলতে সেই প্রতিষ্ঠানকে বোঝায়, যা এজেন্ট ব্যাংকিং কার্যক্রম পরিচালনার জন্য একটি ব্যাংক দ্বারা নিয়োগ করা হয়েছে।

**সাব-এজেন্ট :** সাব-এজেন্ট হলো সেই প্রতিষ্ঠান, যা এজেন্টের অধীনে কাজ করবে এবং একটি নির্দিষ্ট আউটলেটে এজেন্টের ব্যাংকিং কার্যক্রম চালাবে।

#### ১০.৫.১ এজেন্ট/সাব-এজেন্টের জন্য যোগ্য মানদণ্ড

ব্যাংকগুলো নিম্নলিখিত ব্যক্তি / সত্তাকে তাদের এজেন্ট / উপ-এজেন্ট হিসাবে নিয়োজিত করতে পারে—

১. এমএফআই, যারা বাংলাদেশ মাইক্রো ক্রেডিট নিয়ন্ত্রক কর্তৃপক্ষ দ্বারা নিয়ন্ত্রিত।
২. নিবন্ধিত এনজিও।
৩. সমবায় সোসাইটি আইন, ২০০১-এর অধীনে গঠিত এবং নিয়ন্ত্রিত/কোপারেটিভ সোসাইটি।
৪. ডাকঘর।
৫. কুরিয়ার এবং মেলিং সেবা প্রদানকারী সংস্থা, যা পোস্ট ও টেলিযোগাযোগ মন্ত্রণালয়ের অধীনে নিবন্ধিত।
৬. কোম্পানি আইন, ১৯৯৪' এর অধীনে নিবন্ধিত সংস্থাগুলো।
৭. স্থানীয় সরকার প্রতিষ্ঠানের গ্রামীণ ও শহরে অফিস।
৮. মোবাইল নেটওয়ার্ক অপারেশনগুলোর এজেন্ট।
৯. ইউনিয়ন তথ্য ও পরিষেবা কেন্দ্র (ইউআইএসসি)।
১০. শিক্ষিত ব্যক্তিরা যারা IT ভিত্তিক আর্থিক পরিষেবাগুলো চালাতে সক্ষম, বীমা সংস্থাগুলোর এজেন্ট, ফার্মেসিগুলোর মালিক, চেইন শপ এবং পেট্রোল পাম্প/ গ্যাস স্টেশন।

#### ১০.৫.২. এজেন্ট/সাব-এজেন্টদের জন্য যোগ্যতা

- পর্যাপ্ত নগদ এবং অ্যাকাউন্ট ব্যালেন্স বজায় রাখার ক্ষমতা।
- গ্রামীণ গ্রাহকদের সেবা দেওয়ার মতোন প্রোফাইল।

- নতুন ব্যবসায়িক প্রয়োজনে বিনিয়োগের ক্ষমতা।
- বয়স, শিক্ষা এবং স্বত্বাধিকারী/মালিকের অভিজ্ঞতা।
- কৌশলগত অবস্থান।
- ব্যাংক/এটিএমের থেকে দূরত্ব।
- এলাকায় বিশ্বাসযোগ্যতা।
- এলাকায় ব্যবসায়ের সুনাম।
- সামাজিক প্রভাব।
- সামাজিক গ্রহণযোগ্যতা।
- জনশক্তি সমর্থন এবং শিক্ষিত কর্মী।
- নতুন প্রডাক্টের প্রতি এজেন্টদের আগ্রহ।
- আইটি সরঞ্জাম ব্যবহারে অভিজ্ঞতা।

**১০.৬. বাংলাদেশে এজেন্ট ব্যাংকিং সেবা**

- অ্যাকাউন্ট খোলা (সঞ্চয়ী, কারেন্ট, ডিপিএস, এফডিআর ইত্যাদি)।
- নগদ জমা এবং নগদ তোলা।
- অভ্যন্তরীণ বিদেশি রেমিট্যান্স বিতরণ।
- লোন সোর্সিং, বিতরণ এবং রিপেমেন্ট সংগ্রহ করা।
- বিল/ইউটিলিটি বিল সংগ্রহ।
- বীমার প্রিমিয়াম সংগ্রহ।
- অবসর ভাতা এবং সামাজিক সুবিধা প্রদান।
- বেতন প্রদান।
- তহবিল স্থানান্তর।
- এটিএম থেকে টাকা তোলা।
- ব্যালেন্স চেক করা।
- ব্যাংক স্টেইটম্যান্ট তৈরি ও সরবরাহ করা।
- অ্যাকাউন্টের সঙ্গে সম্পর্কিত নথি সংগ্রহ।
- অ্যাকাউন্ট খোলার ফর্ম, লোনের আবেদন ফর্ম, ক্রেডিট এবং ডেবিট কার্ড অ্যাপ্লিকেশন সংগ্রহ করা।
- ব্যাংক কর্তৃক অনুমোদিত লোনের মনিটরিং করা ও তা আদায় করা।
- বাংলাদেশ ব্যাংক কর্তৃক সময়ে সময়ে জারি করা যেকোনো কার্যাবলি।

**১০.৭. এজেন্ট আউটলেটে লেনদেন প্রক্রিয়া**

এজেন্ট আউটলেটগুলো থেকে চেকের মাধ্যমে টাকা তোলা ও বৈদেশিক মুদ্রায় লেনদেন করা ব্যতীত সমস্ত ধরনের লেনদেন করার অনুমতি এজেন্ট আউটলেটগুলোকে দেওয়া হয়। সমস্ত ধরনের লেনদেন করার জন্য এজেন্টকে অবশ্যই তার অ্যাকাউন্টে ভার্চুয়াল অর্থ বজায় রাখতে হবে। যখন কোনো গ্রাহক তার অ্যাকাউন্টে অর্থ জমা দিতে আসে, এজেন্ট তখন নগদ অর্থ গ্রহণ করে এবং তার অ্যাকাউন্ট থেকে সমপরিমাণ অর্থ গ্রাহকের অ্যাকাউন্টে স্থানান্তর করে। একইভাবে, গ্রাহকের অ্যাকাউন্ট থেকে টাকা উত্তোলনের সময় গ্রাহক ফিঙ্গারপ্রিন্ট ব্যবহার করে তার অ্যাকাউন্ট ডেবিট করে সমপরিমাণ অর্থ এজেন্টের অ্যাকাউন্টে স্থানান্তর করেন এবং এজেন্ট নগদ অর্থ গ্রাহককে প্রদান করেন। উল্লেখ্য, এজেন্ট তার ওয়ালেট বা গ্রাহকের অ্যাকাউন্ট উভয়ই তহবিল স্থানান্তর, বিল পেমেন্ট এবং অন্য কোনো লেনদেনের জন্য ব্যবহার করতে পারেন, তবে গ্রাহকের অ্যাকাউন্টের ক্ষেত্রে গ্রাহক ফিঙ্গারপ্রিন্ট প্রদান করবেন। এজেন্ট আউটলেট এর অ্যাকাউন্টগুলোর ভার্চুয়াল অর্থ শেষ হয়ে গেলে তাকে ব্যাংকের শাখা বা ডিস্ট্রিবিউটরের কাছে নগদ অর্থ জমা দিয়ে তার অ্যাকাউন্টটির ভারসাম্য বজায় রাখতে পারেন।

**১০.৮. এজেন্ট আউটলেট থেকে এজেন্ট ব্যাংকিং গ্রাহকের জন্য অপারেশনাল সীমা** (বাংলাদেশ ব্যাংক কর্তৃক নিয়ন্ত্রিত)।

- ব্যাংকগুলো এজেন্টের মাধ্যমে লেনদেনের একটি সীমা নির্ধারণ করে দেয়।
- ব্যাংকগুলো কর্তৃক নির্ধারিত সীমার মধ্যে এজেন্ট লেনদেন করবে।
- এজেন্ট ব্যাংকের সঙ্গে একটি কারেন্ট অ্যাকাউন্ট খুলবে এবং ব্যাংক কর্তৃক নির্ধারিত পরিমাণ টাকা তাতে জমা করবে। প্রাথমিক জমার পরিমান প্রতিটি আউটলেটের জন্য ২ লাখ টাকার চেয়ে কম হওয়া উচিত নয়। এজেন্টের চাহিদা এবং লেনদেনের প্রোফাইলের ভিত্তিতে এই জাতীয় সীমা পুনঃনির্ধারণ করা হবে।
- এজেন্ট অ্যাকাউন্ট তার হিসাবে ন্যূনতম ব্যালেন্সের সম্মত স্তরে যতটা ঘন ঘন সম্ভব রিফিলিংয়ের ব্যবস্থা করবে, তবে, মাসে কমপক্ষে দু'বারের চেয়ে কম নয়; একবার মাসের অর্ধেক পথে এবং অন্যটি মাসের শেষে।
- ব্যাংকগুলো অপ্রত্যাশিত লেনদেনের প্রয়োজনীয়তা পূরণের জন্য এজেন্টের কাছে ক্রেটিড সুবিধাও প্রদান করতে পারে, যা ব্যাংকের সঙ্গে এজেন্টের রক্ষিত ডিপোজিটের ১০০% এর বেশি হবে না।
- সাধারণভাবে, এজেন্ট কর্তৃক পরিচালিত সর্বাধিক সংখ্যা এবং লেনদেনের পরিমাণ নিম্নলিখিত সারণিতে বর্ণিত সীমা অতিক্রম করবে না—

| লাখ টাকায় পরিমাণ | | | | | | |
|---|---|---|---|---|---|---|
| লেনদেনের দৈনিক সংখ্যা এবং পরিমাণের সীমা | | | | | | |
| অ্যাকাউন্টের প্রকৃতি/ধরন | নগদ আমানত | | নগদ উত্তোলন | | স্থানান্তর/ BEFTN/আন্তঃ-ব্যাংক/অন্য ব্যাংকে প্রেরণ | |
| | লেনদেনের সংখ্যা | মোট পরিমাণ | লেনদেনের সংখ্যা | মোট পরিমাণ | লেনদেনের সংখ্যা | মোট পরিমাণ |
| চলতি হিসাব | ৪ | ৬.০০ | ২ | ৫ | ৪ | ১৫.০০ |
| সঞ্চয়ী হিসাব | ২ | ৪.০০ | ২ | ৩ | ২ | ৫.০০ |
| স্পেশাল নোটিশ ডিপোজিট (এসএনডি) | ৪ | ৬.০০ | ২ | ৩ | ৪ | ১০.০০ |

- নির্ধারিত সীমার বাইরেও লেনদেন করা যেতে পারে, তবে এর জন্য এজেন্টের মাধ্যমে ব্যাংককে কমপক্ষে ১ (এক) কার্যদিবসের পূর্বে জানাতে হবে।
- বিশেষ ক্ষেত্রে, যখন সীমা অতিক্রম করে নিয়মিত ব্যাংকিং লেনদেনের প্রয়োজন হয়, তখন ব্যাংকগুলো ব্যাংকের ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী অফিসারের কাছ থেকে যথাযথ অনুমোদন নিয়ে সেই ক্লায়েন্টের জন্য একটি বর্ধিত সীমা নির্ধারণ করতে পারে। বৃদ্ধি অবশ্যই বিচক্ষণ এবং যুক্তিযুক্ত হতে হবে এবং গ্রাহকের যথাযথ অধ্যবসায়, ক্লায়েন্টের চাহিদা এবং সংশ্লিষ্ট ঝুঁকির ওপর ভিত্তি করে তা নির্ধারণ করতে হবে। লেনদেনের সীমা বৃদ্ধির ৩০ (ত্রিশ) দিনের মধ্যে, ব্যাংক বাংলাদেশ ব্যাংকের FID-কে লিখিতভাবে এই ধরনের বৃদ্ধির যৌক্তিকতাসহ কমপক্ষে গত এক মাসের ক্লায়েন্টের লেনদেনের সম্পর্কিত তথ্যসহ অবহিত করতে হবে।

### ১০.৯ এজেন্ট ব্যাংকিংয়ের অনন্য সেলিং প্রপজিশন

- বার্ষিক অ্যাকাউন্ট রক্ষণাবেক্ষণ চার্জ নেই
- ই-পিওএস (E-POS) ব্যবহার করে ডোরস্টেপ সার্ভিস সুবিধা।
- এজেন্ট আউটলেট দ্বারা ইনওয়ার্ড রেমিট্যান্স প্রদান ইতোমধ্যে সব উপজেলা কভার করা হয়েছে।
- ব্যাংকের শাখা, এটিএম, এজেন্ট আউটলেটসহ সব চ্যানেলে দেশব্যাপী লেনদেন সুবিধা।
- গ্রাহক পরিষেবা এবং আউটলেট পর্যবেক্ষণের জন্য নিবেদিত ব্যাংক কর্মকর্তা।
- বিজনেস মডেলের কারণে চ্যানেলের ওপর আরও নিয়ন্ত্রণ।
- মাস্টার এজেন্টের মাধ্যমে ২৪/৭ রিব্যালেন্সিং সুবিধা, বিশেষ করে প্রত্যন্ত অঞ্চলে।
- ৩৬৫ দিন খোলা এবং ব্যাংকিং সময়ের বাইরেও লেনদেনের সুবিধা।

### ১০.১০. এজেন্ট/এজেন্ট আউটলেটগুলোর আরওআই (ROI)

এজেন্ট ব্যাংকিং উদ্যোক্তাদের জন্য একটি লাভজনক ব্যবসায়ের সুযোগ খুলে দেয়। সাধারণত ব্যাংকগুলো আউটলেট দ্বারা সংগৃহীত আমানত সংগ্রহ এবং আউটলেট / উপ-এজেন্টদের দ্বারা লোন বিতরণে তাদেরকে একটি নির্দিষ্ট কমিশন দিয়ে থাকে। তদতিরিক্ত, এজেন্ট আউটলেট প্রতিটি লেনদেন যেমন জমা, উত্তোলন, তহবিল স্থানান্তর, ইউটিলিটি পেমেন্ট, অভ্যন্তরীণ বিদেশি রেমিট্যান্স বিতরণ ইত্যাদি এর জন্য একটি নির্দিষ্ট পরিমাণ চার্জ গ্রহণ করে। তারা প্রতিটি অ্যাকাউন্ট খোলার জন্য একটি কমিশনও পান। তবে উপ-এজেন্টস/আউটলেটগুলোকে তাদের অফিসের ভাড়া, তাদের নিজস্ব কর্মকর্তাদের বেতন এবং ইউটিলিটি ব্যয় বহন করতে হয়। এটি অনুমান করা যায় যে, গ্রামীণ অঞ্চলে ৫ মিলিয়ন এবং নগর অঞ্চলে ১০০ মিলিয়ন ডিপোজিট থাকলে একটি সাব-এজেন্ট বা আউটলেট মাসিক লাভে পরিচালিত হয়।

### ১০.১১ এজেন্ট ব্যাংকিংয়ের চ্যালেঞ্জ

এটি কিছুটা সত্য যে এজেন্ট ব্যাংকিং কিছু চ্যালেঞ্জ তৈরি করেছে যা নিম্নলিখিত হিসাবে চিত্রিত হতে পারে—

**ক. প্রযুক্তি সম্পর্কিত**

- নির্বাচন কমিশনের পোর্টাল থেকে গ্রাহকের আঙুলের ছাপ যাচাইকরণের ব্যর্থতা।
- ব্যর্থ সার্টিফিকেট এবং পাসপোর্ট যাচাইকরণ প্রক্রিয়া না থাকা।
- বিরামবিহীন ইন্টারনেট সংযোগের অভাব।
- বিদ্যুৎ সরবরাহের বাধা।

- নতুন প্রযুক্তির পর্যায়ক্রমিক মূল্যায়ন
- বৃদ্ধ গ্রাহক এবং ফিল্ড কর্মীদের জন্য ফিঙ্গারপ্রিন্টের ম্যাচিং সমস্যা।

**খ. আর্থিক সাক্ষরতা**

- আর্থিক সাক্ষরতার সচেতনতার অভাব।
- নিরক্ষরতার কারণে কোনো অ্যাকাউন্ট খুলতে না পারা।

**গ. প্রতিযোগিতা আগ্রাসন**

- একাধিক ব্যাংক একক সত্তায় গুরুত্বারোপ করে।
- বিভিন্ন ব্যাংকের জন্য বিভিন্ন ধরনের হার।

**ঘ. ব্যাংক ও এজেন্টদের লাভজনকতা**

- হয়ে উঠতে অনেক বেশি সময় লাগে।
- বিভিন্ন ব্যাংক দ্বারা প্রদত্ত একই অঞ্চলে বেশি প্রতিযোগিতা।

**ঙ. গ্রামীণ মানুষের মানসিকতা**

- গ্রামীণ অঞ্চলের লোকেরা এখনও ব্যাংকিং ব্যবস্থা সম্পর্কে অসচেতন।
- তাদের মধ্যে যারা কম শিক্ষিত, তারা এজেন্ট ব্যাংকিংয়ের সঙ্গে স্বাচ্ছন্দ্য বোধ করেন না।

**চ. নগদ বহন এবং পরিচালনার ঝুঁকি**

- এজেন্টরা প্রায়শই নিজেরা নগদ বহন করার সময় জালিয়াতির মুখোমুখি হন।

ছ. জালিয়াতি : কোনো কোনো এজেন্ট বেশি ইন্টারেস্ট প্রদানের লোভ দেখায়ে গ্রাহকের FDR করে, কিন্তু তা ব্যাংকে পোস্টিং না করে আত্মসাৎ করে।

## ১১.কল সেন্টার

### ১১.১. কল সেন্টার কী?

কল সেন্টার হলো একটি গ্রাহক টাচ পয়েন্ট, যা ভয়েস কলের মাধ্যমে কোনো কিছু বিক্রয় করা, কোনো বিষয়ে অনুরোধ, অভিযোগ এবং জিজ্ঞাসা গ্রহণ করা এবং তার সমাধান বা উত্তর প্রদান করা হয়।

### ১১.২. কন্টাক্ট সেন্টার কী?

কন্টাক্ট সেন্টার হলো গ্রাহক টাচ পয়েন্ট যা ভয়েস কল, ফ্যাক্স, ইমেইল, চিঠি/কুরিয়ার, এসএমএস, ওয়েব চ্যাট ইত্যাদি একাধিক যোগাযোগ চ্যানেল ব্যবহার করে কোনো কিছু বিক্রয় করা, কোনো বিষয়ে অভিযোগ এবং জিজ্ঞাসা গ্রহণ করা এবং তার সমাধান বা উত্তর প্রদান করা হয়।

### ১১.৩. কল সেন্টার এবং কন্টাক্ট সেন্টারের মধ্যে পার্থক্য

কল সেন্টার এবং কন্টাক্ট সেন্টারের মধ্যে পার্থক্য হ'ল প্রযুক্তির ব্যবহার যা গ্রাহকদের সঙ্গে যোগাযোগের জন্য ব্যবহৃত হচ্ছে। কল সেন্টারে, কেবল ভয়েস কলের মাধ্যমে যোগাযোগ স্থাপন করা হয়। অন্যদিকে, কন্টাক্ট সেন্টারে যোগাযোগের জন্য একাধিক যোগাযোগ চ্যানেল ব্যবহৃত হয়, যেমন ভয়েস কল, ইমেল, ফ্যাক্স, ওয়েব চ্যাট ইত্যাদি।

### ১১.৪. কন্টাক্ট সেন্টারের যোগাযোগের পদ্ধতি

ভয়েস কল : ভয়েস কল হলো ফোন ব্যবহার করে গ্রাহকের সঙ্গে যোগাযোগের ব্যবস্থা। বিভিন্ন ধরনের ভয়েস ক্যারিয়ার যেমন পিএসটিএন, জিএসএম, সিডিএমএ বা ভিওআইপি একটি কন্টাক্ট সেন্টারে যোগাযোগের জন্য ব্যবহৃত হয়। ভয়েস কলগুলো ইনবাউন্ড এবং আউটবাউন্ড উভয় ক্ষেত্রেই ব্যবহৃত হয়। ভয়েস কল ছাড়া কন্টাক্ট সেন্টারে যোগাযোগের জন্য ব্যবহৃত বাকি মাধ্যমগুলোকে মাল্টিমিডিয়া চ্যানেল বলা হয়।

- ওয়েব চ্যাট : ওয়েব চ্যাট এমন একটি পদ্ধতি, যা ডেডিকেটেড চ্যাট সার্ভিসের সাহায্যে ইন্টারনেট ব্যবহার করে অ্যাক্সেস করা যায়। ওয়েব চ্যাট ব্যবহার করে গ্রাহকরা বিশ্বের যে কোনো জায়গা থেকে কন্টাক্ট সেন্টারে অ্যাক্সেস করতে পারেন। যোগাযোগের এই পদ্ধতিটি গ্রাহকদের জন্য গুরুত্বপূর্ণ যারা প্রায়শই বিভিন্ন ভৌগোলিক অবস্থান জুড়ে ঘুরে বেড়ান।
- কমিউনিটি সার্ভিস/ফোরাম/ব্লগ : কন্টাক্ট সেন্টারের বর্তমান যুগের টুলস্ হল কমিউনিটি সার্ভিস, ফোরাম, ব্লগ ইত্যাদি। এই টুলস্গুলো অন্যান্য গ্রাহকের আলোচনা, মতামত ও অভিজ্ঞতাকে উৎসাহিত করতে সাহায্য করে। কন্টাক্ট সেন্টারের পক্ষ থেকে এজেন্ট আলোচনার দিকনির্দেশনা প্রদান করে, বিষয়টি শুরু করে এবং সমাধান প্রদান করে। প্রযুক্তিগত সেবা প্রদানকারী কন্টাক্ট সেন্টারের জন্য এই পদ্ধতি খুবই উপযোগী।
- ই-মেইল : ই-মেইল মাল্টিমিডিয়া জাতীয় যোগাযোগের একটি মাধ্যম। যোগাযোগের এই মাধ্যমটি সাধারণত অফ-লাইনে গ্রাহককে সেবা প্রদানের

জন্য ব্যবহৃত হয়। এটি প্রায়শই আন্তর্জাতিক কন্টাক্ট সেন্টারে যোগাযোগের জন্য ব্যবহৃত হয়।

- এসএমএস : এসএমএস প্রায়শই ঐসব কন্টাক্ট সেন্টারে ব্যবহৃত হয় যেখানে ভোট, জনমত, পুশ-পুল সেবা প্রদান করা হয়। এসএমএস হলো কম খরচে গ্রাহককে তথ্য সরবরাহের একটি কার্যকর টুলস্।
- ফ্যাক্স : ফ্যাক্স সরাসরি কাগজ প্রক্রিয়াকরণের বিকল্প হিসাবে ব্যবহৃত হয় যেমন, কোনো নির্দিষ্ট ইস্যুতে গ্রাহকের অনুমোদন পেতে সরাসরি কাগজে স্বাক্ষর না নিয়া ফ্যাক্সের মাধ্যমে তা গ্রহণ করা। দুটি ধরনের ফ্যাক্স কন্টাক্ট সেন্টারে ব্যবহার করা হয়। (১) ট্রেডিশনাল ফ্যাক্স এবং (২) ই-ফ্যাক্স।
- চিঠি/কুরিয়ার, ডাক : একটি কন্টাক্ট সেন্টার যেখানে কাগজ প্রক্রিয়াকরণের প্রয়োজন হয়, সেখানে এই যোগাযোগের মাধ্যমটি ব্যবহারের জন্য উপযুক্ত। আইনি সেবা, সাধারণ গ্রাহক পরিষেবা এবং যেখানে সাক্ষরতার হার কম থাকে সেখানে যোগাযোগের এই মাধ্যমটি কন্টাক্ট সেন্টারে উল্লেখযোগ্যভাবে ব্যবহৃত হয়।

## ১১.৫. কন্টাক্ট সেন্টারের মূল উপাদানগুলো

### ১১.৫.১. ইন্টারেক্টিভ ভয়েস রেসপন্স (আইভিআর)

আইভিআর একটি বুদ্ধিমান উপায়ে কলগুলো পরিচালনা করে যেখানে গ্রাহক ইনপুট দিতে পারে এবং স্বয়ংক্রিয়ভাবে ব্যাংকিং সিস্টেমগুলো থেকে তিনি স্ট্যাটিক ও ডায়নামিক আউটপুট পেতে পারেন। এখানে, আইভিআর একটি কোয়ারি বিশ্লেষক হিসাবে কাজ করে। তাছাড়া আইভিআর গ্রাহককে এজেন্টের সঙ্গে কথা বলার জন্যও সুযোগ দেয়। যদি কোনো গ্রাহক এজেন্টের সঙ্গে কথা বলতে চান তবে আইভিআর এসিডি-তে কলটি হস্তান্তর করে।

### ১১.৫.২ স্বয়ংক্রিয় কল ডিস্ট্রিবিউটর (এসিডি)

এসিডি কিছু নির্ধারিত সেটিংয়ের ওপর ভিত্তি করে কলগুলোকে এজেন্টের কাছে পাঠায়। এতে একটি বিল্ট-ইন ইনটেলিজেন্ট সিস্টেম ব্যবহার করা হয়। সাধারন লজিক হলো, সবচেয়ে বেশি সময় ধরে নিষ্ক্রিয় এজেন্টের কাছে কলটি প্রেরন করা।

### ১১.৫.৩. কম্পিউটার টেলিফোনি ইন্টিগ্রেশন (সিটিআই)

এসিডি কলটি তখন সিটিআই-এর কাছে প্রেরণ করে। সিটিআই পূর্বনির্ধারিত সংখ্যা অনুযায়ী বিভিন্ন ব্যাংকিং সিস্টেম থেকে গ্রাহকের প্রাসঙ্গিক তথ্যাবলি এজেন্টের সামনে প্রদর্শন করে। ঐ তথ্যের ভিত্তিতে এজেন্ট গ্রাহককে প্রয়োজনীয় তথ্য প্রদান করে সাহায্য করেন।

### ১১.৫.৪. কল রেকর্ডিং সিস্টেম

এজেন্ট এবং গ্রাহকের মধ্যে সমস্ত ভয়েস কল এবং স্ক্রিন সট রেকর্ড করা হয়। ব্যাংকিং কল সেন্টারগুলোর জন্য ১০০% কল রেকর্ড করা হয়।

### ১১.৫.৫. স্টাফ (এজেন্ট / সুপারভাইজার)

কন্টাক্ট সেন্টারের মূল সম্পদ স্পষ্টতই এর মানবসম্পদ। যে ব্যক্তি সরাসরি গ্রাহকদের পরিবেশন করে তিনি 'এজেন্ট' হিসাবে পরিচিত যদিও তাদের অবশ্যই আলাদা এইচআর উপাধি থাকতে হবে, যা তাদের ভিজিটিং কার্ডগুলোতে ব্যবহৃত হয়। একটি কন্টাক্ট সেন্টারের এজেন্টের খুব ভালো ভয়েস থাকা উচিত, উচ্চ শ্রবণশক্তি, লেখার এবং কথা বলার দক্ষতা থাকতে হবে। কন্টাক্ট সেন্টারের কাজে সাফল্যের প্রধান শর্ত হল এজেন্টকে ভীষণ ধৈর্যশীল হতে হবে এবং তার অবশ্যই ইতিবাচক, সক্রিয় এবং সহায়তার মনোভাব থাকতে হবে। কন্টাক্ট সেন্টারের অন্যতম গুরুত্বপূর্ণ বিষয় হলো যে, এজেন্টের প্রয়োজনীয়তার সঠিক সংখ্যা চিহ্নিত করা। বেশ কয়েকটি কারণ এজেন্টের প্রয়োজনীয়তার সংখ্যা নির্ধারণ করে। এই কারণগুলো হলো—

—এক ঘণ্টার মধ্যে কল আগমনের সংখ্যা।
—একটি কলের গড় হ্যান্ডলিং সময়।
—টার্গেট পরিষেবা স্তর।
—টার্গেট কল উত্তর প্রান্তিক সময়।
—শিফটে কর্মরত সময়, একদিনে শিফটের সংখ্যা, এক সপ্তাহের কার্যদিবসের সংখ্যা।
—সঙ্কুচিত (সপ্তাহান্তে এবং বছরে ছুটি, বিভিন্ন ধরনের ছুটির পরিমাণ ইত্যাদি)

সাধারণত এরলং-সি তত্ত্বটি ও ওপরে বর্ণিত তথ্যাবলি ব্যবহার করে প্রয়োজনীয় এজেন্টের সংখ্যা গণনা করা হয়।

সুপারভাইজারের সংখ্যা সাধারণত এজেন্টের সংখ্যা এবং শিফটের সংখ্যা দ্বারা নির্ধারিত হয়। সাধারণত একটি অ-প্রযুক্তি কন্টাক্ট সেন্টারে প্রতি ৮ জন এজেন্টের জন্য ১ জন সুপারভাইজার রাখা হয়। প্রযুক্তিগত কন্টাক্ট সেন্টারের জন্য প্রতি ২ জন এজেন্টের জন্য ১ জন সুপারভাইজার রাখা হয়। সুপারভাইজাররা কন্টাক্ট সেন্টারের অপারেশনে গুরুত্বপূর্ণ ভূমিকা পালন করে। তারা সংস্থাগুলোর সমাধান প্রদানকারী ও সেবা সমন্বয়কারী হিসাবে কাজ করেন।

### ১১.৫.৬. কী পারফরম্যান্স ইন্ডিকেটর (কেপিআই)

কেপিআই দ্বারা যোগাযোগ কেন্দ্রটি চলে, যা ইঙ্গিত করে কীভাবে কন্টাক্ট সেন্টারের এজেন্টরা তাদের সময় ব্যয় করে, তারা কীভাবে পারফর্ম করছে, কোন ধরনের মান বজায় রাখা হচ্ছে, গ্রাহকরা কীভাবে সেবা হচ্ছে, কল শেষ হওয়ার পরে কতজন গ্রাহক সুখী হলেন ইত্যাদি। এসব প্রশ্নের উত্তর কেপিআই-তে পাওয়া যাবে। কন্টাক্ট সেন্টারে KPI দুভাবে সেট করা যায় এজেন্ট পর্যায়ে ও সুপারভাইজার পর্যায়ে। এজেন্ট-লেভেলের কেপিআইগুলো সেবার গতি এবং গুণমানকে প্রভাবিত করে এমন উপাদানগুলো অন্তর্ভুক্ত করা উচিত। অন্যদিকে, সুপারভাইজার পর্যায়ের কেপিআইয়ের মধ্যে এমন উপাদানগুলো অন্তর্ভুক্ত করা উচিত, যা কন্টাক্ট সেন্টারের আউটপুটকে প্রভাবিত করতে পারে যেমন সেবার মান, ASA, FCR ইত্যাদি। একবার কেপিআই ডিজাইন নিখুঁত হয়ে গেলে, গ্রাহক সেবার মান কেবল পরিষেবা বিধানের মাধ্যমেই অর্জন করা যায়।

### ১১.৬. কল সেন্টার / কন্টাক্ট সেন্টার কীভাবে কাজ করে?

**একটি কল সেন্টার/কন্টাক্ট সেন্টারের ফ্লো নিচে বর্ণিত হলো**—

১. গ্রাহক কল সেন্টারের নম্বরে কল করেন।

২. কলটি তার ক্যারিয়ার (যেমন পিএসটিএন, জিএসএম, সিডিএমএ, ভিওআইপি) থেকে বিটিসিএল চ্যানেলে পৌঁছানো হয়।

৩. কলটি তখন SS7 ব্যবহার করে ব্যাংকের সাইড ট্রাঙ্কগুলোতে আনা হয়।

৪. কলটি তখন আইভিআরে অবতরণ করে, যেখানে আইভিআর গ্রাহকের প্রোফাইল এবং তার প্রদত্ত ইনপুট অনুযায়ী গ্রাহককে সেবা দিবে; এই পর্যায়ে গ্রাহক দুটি বিকল্প পাবেন—

i. যদি কোনো গ্রাহক 'Self-Service' নির্বাচন করেন তবে তিনি আইভিআর কর্তৃক সেবা পাবেন। আইভিআর বিভিন্ন ব্যাংকিং সিস্টেম থেকে ডেটা পুনরুদ্ধার করবে এবং গ্রাহকের অনুরোধ অনুযায়ী এটি গ্রাহকের কাছে পড়ে শুনাবে। তাছাড়া আইভিআর গ্রাহক প্রদত্ত নির্দেশাবলিও কার্যকর করবে।

ii. গ্রাহক যদি 'Assisted Service' নির্বাচন করেন তবে—

ক. গ্রাহকের কলটি এসিডিতে স্থানান্তরিত হবে।

খ. আইভিআর থেকে গ্রাহকের প্রোফাইল পাওয়ার পরে, এসিডি গ্রাহকের প্রোফাইলটি পরীক্ষা করে এবং কলটির জন্য একজন উপযুক্ত এজেন্ট নির্বাচন করবে।

গ. তারপরে এসিডি কলটি নির্বাচিত এজেন্টের সিটিআইতে স্থানান্তর করবে (যদি কোনো খালি এজেন্ট না থাকে তবে কোনো এজেন্ট খালি না হওয়া পর্যন্ত কলটি এসিডি-এর কিউ-তে রাখা হবে)

ঘ. খালি এজেন্ট পাওয়া গেলে, ঐ এজেন্টের সিটিআই-তে কলটি প্রেরণ করা হবে এবং এজেন্টের সিটিআই-এ গ্রাহকের বিভিন্ন ডেটা প্রদর্শিত হবে। তাছাড়া এজেন্ট কলটি উত্তর দেওয়া, বাতিল করা, ট্যান্সফার করা বা ফরওয়ার্ড করার অপশন দেখতে পারেন।

ঙ. কলটি শেষ হওয়ার পর, এজেন্ট কলটির কারণ সংক্রান্ত কোডটি নির্বাচন করবেন এবং ডাটাবেসে সেইভ করবেন।

### ১১.৭. কল সেন্টার / কন্টাক্ট সেন্টারের প্রকারভেদ

কল সেন্টার/কন্টাক্ট সেন্টার কোন সংস্থায় দুটি ভিন্ন ধরনের ভূমিকা পালন করতে পারে—

- কেবল আইভিআরের মাধ্যমে 'Self-Service' প্রদান করা যেখানে আইভিআর প্রাসঙ্গিক তথ্য পড়ে শোনায় এবং গ্রাহকের ইনপুট অনুসারে নির্দেশনা সম্পাদন করে।
- 'Assisted Service' প্রদান করে যেখানে মানব এজেন্টরা কলটির উত্তর দেয় এবং প্রয়োজনীয়তাগুলো সম্পাদন করে।

একটি সাধারণ কল সেন্টার/কন্টাক্ট সেন্টারে সাশ্রয়ী কার্যকারিতা নিশ্চিত করার জন্য একই সঙ্গে 'Self-Service' এবং 'Assisted Service' সেবা প্রদান করা যেতে পারে।

'Self-Service' ও 'Assisted Service' নামক সেবাসমূহের বৈশিষ্ট্য ও পার্থক্য নিচে প্রদত্ত হলো—

| প্যারামিটার | Self-Service | Assisted Service |
|---|---|---|
| সার্ভিস ডেলিভারি মোড | • ইন্টারেক্টিভ ভয়েস রেসপন্স (আইভিআর) | • কল সেন্টারের এজেন্ট |
| সাফল্যের মূল কারণ | • আইভিআর এর ফ্লো খুবই সহজ ও সরল।<br>• জনপ্রিয় পরিষেবার প্রাপ্যতা<br>• নিরাপত্তা চেকিং | ▪ আচরণ<br>▪ যোগাযোগ<br>▪ গভীর জ্ঞান<br>▪ যথাসময়ে সমাধান প্রদান |
| কেন এই | • কম-খরচ | ▪ কাস্টমাইজড এবং |

| | | |
|---|---|---|
| টাচপয়েন্ট ব্যবহার করবেন? | • অংশগ্রহণমূলক সেবা প্রদান নিশ্চিত করা<br>• সেবা প্রদানের ঝুঁকি হ্রাস করা<br>• সেবা প্রদানে দক্ষতা বৃদ্ধি<br>• সেবা প্রদানে সর্বদা প্রস্তুত | জটিল সমস্যাগুলো পরিচালনা করা।<br>▪ অভিযোগসমূহ সমাধান করা<br>▪ অসংগঠিত পরিষেবা প্রদান (কোয়েরি ইত্যাদি)।<br>▪ অতি সাধারণ গ্রাহকদের সেবা প্রদান। |

### ১১.৮. কল সেন্টার/কন্টাক্ট সেন্টারের কার্যাবলির ধরন

কার্যকলাপগুলোর ওপর ভিত্তি করে কল সেটার/কন্টাক্ট সেন্টার গ্রুপগুলোকে নিম্নলিখিতভাবে শ্রেণিবদ্ধ করা যায়—

ক. ইনবাউন্ড : শুধু অনুসন্ধান, অনুরোধ/নির্দেশ এবং অভিযোগের জন্য কল গ্রহণ করা হয়।

খ. আউটবাউন্ড : বিক্রয়, সমীক্ষা, পণ্যের প্রচার, সংগ্রহ ইত্যাদির লক্ষ্যে গ্রাহকদের কল করা হয়।

গ. মিশ্র মোড : সেবা, বিক্রয় ইত্যাদির ক্ষেত্রে সর্বোত্তম গ্রাহক সেবা নিশ্চিত করতে এই মোডে ইনবাউন্ড এবং আউটবাউন্ড কার্যক্রম একই সঙ্গে ব্যবহার করা হয়।

### ১১.৮.১. সাধারণ ইনবাউন্ড কার্যক্রম

- অনুসন্ধানের উত্তর প্রদান।
- অভিযোগ নথিভুক্ত করা।
- অনুরোধ গ্রহণ করা।
- আপ এবং ক্রস-সেলিং।
- নতুন পণ্যের প্রচার করা।
- সংশ্লিষ্ট কর্তৃপক্ষের কাছে জটিল সমস্যা উপস্থাপন করা।
- কমিউনিটি সার্ভিস, ব্লগ, ফোরাম ইত্যাদি পরিচালনা করা।

### ১১.৮.২. সাধারণ আউটবাউন্ড কার্যক্রম

- স্বাগতম কল।
- নিয়মিত কল ব্যাক করা।
- বিক্রয় ক্যাম্পেইন পরিচালনা করা।
- আপ এবং ক্রস-সেলিং করা।
- বিশেষ ক্যাম্পেইন করা।
- তথ্য সংগ্রহ এবং ডেটা এন্ট্রি করা।
- গ্রাহক প্রতিক্রিয়া/সন্তুষ্টি সংক্রান্ত সমীক্ষা করা।
- নতুন পণ্যের প্রচার করা।
- কালেকশন।
- রিটেনশন।

### ১১.৯. কন্টাক্ট/কল সেন্টারে কোয়ালিটি অ্যাসুরেন্স

গুণমান নিশ্চয়তা (কোয়ালিটি অ্যাসুরেন্স) হলো সার্ভিস ডেলিভারি সিস্টেম ও প্রক্রিয়ার মনিটরিং, মূল্যায়ন এবং নিয়ন্ত্রণ করার একটি প্রক্রিয়া—যাতে সেবাগুলো নির্ধারিত মানের কি না তা নিশ্চিত করা যায়। কোয়ালিটি অ্যাসুরেন্সের বৈশিষ্ট্যসমূহ নিম্নরুপ—

- সেবা প্রদান প্রক্রিয়ার মান নির্ধারণ করা।
- সার্ভিস মূল্যায়ন প্রক্রিয়া সংজ্ঞায়িত করা।
- প্রদেয় সার্ভিসের মনিটরিং ও মূল্যায়ন।
- প্রদেয় সার্ভিসের মান সম্পর্কে এজেন্ট, সুপারভাইজার এবং ব্যবস্থাপনার কাছে ফিডবেক প্রদান।
- প্রশিক্ষণের জন্য সুপারিশ করা।
- সেবা সংক্রান্ত অভিযোগ সমূহের তদন্ত করা।
- গুরুত্বপূর্ণ সার্ভিস ফ্যাক্টর ও ঘটনাসমূহ হাইলাইট করা।
- প্রক্রিয়ার উন্নতি এবং পরিবর্তনের জন্য সুপারিশ করা।
- এজেন্টদের পণ্য এবং সিস্টেম সম্বন্ধে জ্ঞান হালনাগাদ করা।
- দৈনিক ক্লিনিং পরিচালনা করা।

## ১২. তহবিল স্থানান্তর নির্দেশ পাঠানোর জন্য সিস্টেমসমূহ

### ১২.১. টেলেক্স (Telex)

বাংলাদেশের ব্যাংকগুলো টেলিক্সের মাধ্যমে বিদেশি বা স্থানীয় ব্যাংকে তহবিল স্থানান্তর বা এলসি-সম্পর্কিত তথ্য পাঠাতে এবং গ্রহণ করতে ব্যবহৃত হতো। কিন্তু বর্তমানে টেলেক্স-এর পরিবর্তে ব্যাংকগুলো সুইফট ব্যবহার করছে। তার অনেকগুলো কারণ রয়েছে। এইগুলো হলো—

ক. টেলেক্স বার্তাগুলো সুরক্ষিত নয়। এটি বিশ্বের যে কোনো জায়গায় অবস্থিত যে কোনো মেশিন থেকে পাঠানো যায়। টেলেক্স বার্তাগুলোর নিরাপত্তার জন্য একটি 'Test Key' ব্যবহার করা হয়। তারপরও টেলেক্স থেকে

প্রতারণামূলক বার্তা প্রেরণের মাধ্যমে বেশ কয়েকটি প্রতারণার ঘটনা ঘটেছে। সুইফট-এর ক্ষেত্রে, শুধু একজন অনুমোদিত সুইফট সদস্য একটি বার্তা প্রেরণ করতে পারেন। প্রতিটি বার্তার একটি পরিচয় থাকে, যা নির্দেশ করে যে এটি কোথা থেকে এসেছে এবং এইভাবে প্রেরককে প্রতারণার যেকোনো ঘটনার জন্য দায়ী করা যেতে পারে।

খ. টেলেক্স কখনও কখনও গার্বেজ বার্তা তৈরি করে যার জন্য ব্যাংকগুলো প্রেরককে বার্তাটি পুনরায় প্রেরণের জন্য অনুরোধ করে। এতে সময় ও ব্যয়ের অপচয় হয়।

গ. সুইফটের মাধ্যমে বার্তা প্রেরণ, টেলেক্সের মাধ্যমে প্রেরণের চেয়ে সস্তা।

ঘ. বিশ্বের ৯০% ব্যাংক সুইফট ব্যবহার করছে। তাদের ব্যাংকিং অ্যাপ্লিকেশন সফ্‌টওয়্যারটি সুইফট ফর্ম্যাটে বার্তা তৈরি করতে এবং ম্যানুয়াল হস্তক্ষেপ ছাড়াই গন্তব্যে পাঠাতে সক্ষম। এছাড়াও, এই অ্যাপ্লিকেশন সফ্‌টওয়্যারগুলো একটি দেশি বা বিদেশি ব্যাংক থেকে সুইফট দ্বারা প্রাপ্ত বার্তা পড়তে পারে এবং ভাউচারগুলোর স্বয়ংক্রিয়ভাবে পোস্টিং হয়ে যায়। এবং বিভিন্ন চিঠি, প্রতিবেদন এবং বিবৃতি স্বয়ংক্রিয়ভাবে প্রস্তুত করা হয়। ফলে টেলেক্সের মাধ্যমে বার্তা পাঠাতে বা টেলেক্সের মাধ্যমে প্রাপ্ত বার্তাগুলোর আরও প্রক্রিয়াকরণের জন্য ব্যাংকগুলোর অতিরিক্ত জনবলের প্রয়োজন হয়। ফলে টেলিক্সের মাধ্যমে যোগাযোগের জন্য তারা বিদেশি ব্যাংকগুলোর কাছে অতিরিক্ত চার্জ আদায় করে। বর্তমানে কোনো ব্যাংকই এই ধরনের যোগাযোগ গ্রহণ করে না, এমনকি অতিরিক্ত চার্জ দিয়েও।

## ১২.২.সুইফট (SWIFT)

### ১২.২.১. সুইফট কী?

সুইফট এর সংক্ষিপ্ত রূপ 'সোসাইটি ফর ওয়ার্ল্ডওয়াইড ইন্টারব্যাংক ফিন্যান্সিয়াল টেলিকমিউনিকেশন'।

এটি বেলজিয়ামভিত্তিক একটি ব্যাংক-মালিকানাধীন কো-অপারেটিভ, যা বিশ্বব্যাপী আর্থিক সম্প্রদায়কে সেবা প্রদান করে। সুইফট ২০ বছর আগে আত্মপ্রকাশ করেছিল এবং এখন এটি ১৭৮টি দেশের ৬,৪৯৫টি ব্যাংক এবং আর্থিক প্রতিষ্ঠানকে নিরাপদ মেসেজিং সার্ভিসসহ ২৪-ঘণ্টা বিশ্বব্যাপী সাপোর্ট সার্ভিস প্রদান করে যাচ্ছে। সুইফটের গ্লোবাল নেটওয়ার্ক দিনে গড়ে ৪ মিলিয়ন বার্তা বহন করে। সুইফট নেটওয়ার্কে অর্থপ্রদানের বার্তাগুলোর গড় দৈনিক মূল্য ২ ট্রিলিয়ন ডলারের ওপরে অনুমান করা হয়। সুইফট তার গ্রাহকদের খরচ কমাতে, অটোমেশন উন্নত করতে এবং ঝুঁকি পরিচালনা করতে সাহায্য করে। আজ এর ৩,০০০ সদস্য ব্যাংকা ছাড়াও সুইফট ব্যবহারকারীদের মধ্যে উপ-সদস্য এবং অংশগ্রহণকারীরা যেমন ব্রোকার, ইনভেস্টমেন্ট ম্যানেজার, সিকিউরিটিজ ডিপোজিটর এবং ক্লিয়ারিং সংস্থা এবং স্টক এক্সচেঞ্জ রয়েছে।

### ১২.২.২. সুইফট ট্রাফিক

২৯ অক্টোবর ১৯৯৮-এ সুইফটের গড় দৈনিক ট্রাফিক ছিল ৩.৯৫ মিলিয়ন বার্তা যার মধ্যে সর্বোচ্চ ট্রাফিক বার্তা ছিল ৪.২৮ মিলিয়ন। সুইফটের ট্রাফিক আর্থিক বাজারের বিস্তৃত পরিসরে কাজ করে, যার মধ্যে রয়েছে পেমেন্ট (৬৪.৪%), সিকিউরিটিজ (২৮.৯%), ট্রেজারি (১০.২%), ট্রেড ফাইন্যান্স (৫.৮%), এবং অন্যান্য (২.৯%)। সুইফটের ট্রাফিক ইউরোপ, মধ্যপ্রাচ্য এবং আফ্রিকা অঞ্চলের (৬০.৬%) পর আমেরিকা (২০.১%) এবং এশিয়া-প্যাসিফিক (১৫.২%) অঞ্চলে বেশি। তবে ইউএসএ-তে কর্মরত সব গ্রাহকের পাঠানো ট্রাফিকের পরিমাণ সবচেয়ে বেশি এবং তার পরে রয়েছে ইউকে এবং জার্মানি। রুটগুলোর মধ্যে যুক্তরাজ্য এবং মার্কিন যুক্তরাষ্ট্রের মধ্যের রুটটি সর্বাধিক সংখ্যক ট্রাফিক বহন করে।

### ১২.২.৩. সুইফট সদস্যপদ

সুইফট সদস্যদেরকে তিনটি বিভাগে ভাগ করা যায়, যেমন—

#### ক. সদস্য

আন্তর্জাতিক আর্থিক বার্তা প্রেরণের সঙ্গে জড়িত যে কোনো সংস্থা সুইফটের সদস্য হতে পারে, যেমন ডাচ্-বাংলা ব্যাংক এর সদস্য হতে পারে। ফলে বাংলাদেশে ডাচ্-বাংলা ব্যাংক এর সমস্ত শাখার লেটার অফ ক্রেডিট (এল/সি) এবং অন্যান্য বার্তা যেমন ফান্ড ট্রান্সফারের জন্য সুইফট ব্যবহার করতে পারে। সদস্যরা সুইফট-এর শেয়ারহোল্ডার, ফলে তাদের ভোটাধিকার রয়েছে। সদস্য ব্যাংককে একটি ৮-সংখ্যার BIC (ব্যাংক আইডেন্টিফিকেশন নম্বর) বরাদ্দ করা হয় যেমন ডাচ্-বাংলা ব্যাংকের জন্য 'DBBL BD DH' যেখানে BD মানে বাংলাদেশ এবং DH মানে ঢাকা। BIC-এর সঙ্গে তিনটি সংখ্যা যোগ করে শাখা চিহ্নিত করা হবে। উদাহরণস্বরূপ, ডাচ্-বাংলা ব্যাংকের লোকাল অফিস এবং আগ্রাবাদ শাখার BIC হল যথাক্রমে 'DBBL BD DH 101' এবং 'DBBL BD DH 102'।

#### খ. উপ সদস্য

উপ-সদস্যরা হয় একটি পৃথক সংস্থা, যা কমপক্ষে প্রত্যক্ষভাবে ৯০% বা পরোক্ষভাবে ১০০% একজন সদস্যের মালিকানাধীন, বা সদস্য প্রতিষ্ঠানের বিদেশি শাখা। উদাহরণস্বরূপ, যদি ডাচ্-বাংলা ব্যাংকের ইউএসএ-তে একটি শাখা

থাকে, তাহলে সেই শাখাটি সুইফট অ্যাক্সেস করতে পারবে না, যদি না এটি উপ-সদস্য পদ গ্রহণ না করে।

**(গ) অংশগ্রহণকারী**

অংশগ্রহণকারীরা সাধারণত নিম্নলিখিত কোম্পানিগুলোর মধ্যে একটি—

i সিকিউরিটিজ এবং আর্থিক উপকরণ সম্পর্কিত ব্রোকার ও ডিলার।
ii সিকিউরিটিজ এবং সম্পর্কিত আর্থিক উপকরণ সম্পর্কিত স্বীকৃত এক্সচেঞ্জ।
iii সেন্ট্রাল ডিপোজিটরি এবং ক্লিয়ারিং প্রতিষ্ঠান।
iv মানি ব্রোকার।
v ট্রাস্ট বা ফিডোসারি সেবা সংস্থাগুলো।
vi কাস্টোডি ও নমিনী সেবা প্রদানকারীর সাবসিডিয়ারি।
vii রেজিস্ট্রার এবং ট্রান্সফার এজেন্ট সংস্থা।
viii বিনিয়োগ ব্যবস্থাপনা প্রতিষ্ঠান।
ix পেমেন্ট সিস্টেমে অংশগ্রহণকারীরা।
x ট্রেভেলার্স চেক ইস্যুকারী।
xi ট্রেডিং ইনস্টিটিউট।
xii সিকিউরিটিজ ইলেকট্রনিক ট্রেড কনফার্মেশন (ETC) সেবা প্রদানকারী।
xiii একটি ব্যাংকের প্রতিনিধি অফিস বা ব্যাংকগুলোর একটি কনসোর্টিয়াম।
xiv নন-শেয়ারহোল্ডিং ব্যাংক।
xv নন-শেয়ারহোল্ডিং আর্থিক প্রতিষ্ঠান এবং
xvi নিরাপত্তা প্রক্সি ভোটিং সংস্থা।

### ১২.২.৪. কেন সুইফট সদস্য হতে হবে?

বাংলাদেশের ব্যাংকগুলো টেলিক্সের মাধ্যমে একটি বিদেশি ব্যাংকে/থেকে তহবিল স্থানান্তর বা এল/সি-সম্পর্কিত তথ্য পাঠাতে এবং গ্রহণ করতে ব্যবহৃত হয়। টেলেক্স-এর পরিবর্তে ব্যাংকগুলোকে সুইফট ব্যবহার করার জন্য অনেকগুলো কারণ রয়েছে। এগুলো হলো—

ক. টেলেক্স বার্তাগুলো সুরক্ষিত নয়। এটি বিশ্বের যে কোনো জায়গায় অবস্থিত যে কোনো মেশিন থেকে পাঠানো যায়। টেলেক্স বার্তাগুলোর নিরাপত্তার জন্য একটি 'Test Key' ব্যবহার করা হয়। তারপরও টেলেক্স থেকে প্রতারণামূলক বার্তা প্রেরণের মাধ্যমে বেশ কয়েকটি প্রতারণার ঘটনা ঘটেছে। সুইফট-এর ক্ষেত্রে, শুধু একজন অনুমোদিত সুইফট সদস্য একটি বার্তা প্রেরণ করতে পারেন। প্রতিটি বার্তার একটি পরিচয় থাকে, যা নির্দেশ করে যে এটি কোথা থেকে এসেছে এবং এইভাবে প্রেরককে প্রতারণার যেকোনো ঘটনার জন্য দায়ী করা যেতে পারে।

খ. টেলেক্স কখনও কখনও গার্বেজ বার্তা তৈরি করে, যার জন্য ব্যাংকগুলো প্রেরককে বার্তাটি পুনরায় প্রেরণের জন্য অনুরোধ করে। এতে সময় ও ব্যয়ের অপচয় হয়।

গ. বিশ্বের ৯০% ব্যাংক সুইফট ব্যবহার করছে। তাদের ব্যাংকিং অ্যাপ্লিকেশন সফ্টওয়্যারটি সুইফট ফর্ম্যাটে বার্তা তৈরি করতে এবং ম্যানুয়াল হস্তক্ষেপ ছাড়াই গন্তব্যে পাঠাতে সক্ষম। এছাড়াও এই অ্যাপ্লিকেশন সফ্টওয়্যারগুলো একটি দেশি বা বিদেশি ব্যাংক থেকে সুইফট দ্বারা প্রাপ্ত বার্তা পড়তে পারে এবং ভাউচারগুলোর স্বয়ংক্রিয়ভাবে পোস্টিং হয়ে যায়। এবং বিভিন্ন চিঠি, প্রতিবেদন এবং বিবৃতি স্বয়ংক্রিয়ভাবে প্রস্তুত করা হয়। ফলে টেলেক্সের মাধ্যমে বার্তা পাঠাতে বা টেলেক্সের মাধ্যমে প্রাপ্ত বার্তাগুলোর আরও প্রক্রিয়াকরণের জন্য ব্যাংকগুলোর অতিরিক্ত জনবলের প্রয়োজন হয়। ফলে টেলিক্সের মাধ্যমে যোগাযোগের জন্য তারা বিদেশি ব্যাংকগুলোর কাছে অতিরিক্ত চার্জ আদায় করে। বর্তমানে কোনো ব্যাংকই এই ধরনের যোগাযোগ গ্রহণ করে না, এমনকি অতিরিক্ত চার্জ দিয়েও।

### ১২.২.৫. সুইফট এ নিরাপত্তা

সুইফট বিভিন্ন স্তরের নিরাপত্তা বজায় রাখে। অপারেটর শুধু একটি বার্তা প্রস্তুত করতে পারেন। সুইফট নেটওয়ার্কে বার্তাটি পোস্ট করার আগে, এটি একজন সুপারভাইজার দ্বারা অনুমোদন করতে হয়। সুপারভাইজার প্রতিটি বার্তা সাবধানে পরীক্ষা করে এবং তার পাসওয়ার্ড প্রদান করে তা অনুমোদন করেন। বিভিন্ন কার্যক্রম এবং মূল্যবোধের জন্য একাধিক স্তরের নিরাপত্তা থাকতে পারে। শুধু অনুমোদিত টার্মিনাল (সদস্যের অফিসে কম্পিউটার) সুইফট নেটওয়ার্কের সঙ্গে সংযোগ করতে সক্ষম হয়, অন্য কোন কম্পিউটারের সংযোগ প্রত্যাখ্যান করা হবে। এভাবে কড়া নিরাপত্তা ব্যবস্থা বহাল রাখা হয়।

তাছাড়া সমস্যার সমাধান ও সিস্টেমের রক্ষণাবেক্ষণ কাজের জন্য, দুজন নিরাপত্তা কর্মকর্তাকে মনোনীত করতে হবে—একজন আইটি বিভাগ থেকে এবং একজন আইডি বিভাগ থেকে। তাদেরকে যথাক্রমে নিরাপত্তা পাসওয়ার্ডের পার্ট-১ এবং পার্ট-২ দেওয়া হবে। যদি কোনো সমস্যার সমাধান বা রক্ষণাবেক্ষণের কাজের প্রয়োজন হয়, উভয় কর্মকর্তাকে একসঙ্গে পাসওয়ার্ড ব্যবহার করে কাজ করতে হয়।

### ১২.২.৬. সুইফট কীভাবে কাজ করে?

সুইফট মূলত X.25 পাবলিক সুইচ ডেটা নেটওয়ার্ক (পিএসডিএন) এর ওপর ভিত্তি করে একটি বিশ্বব্যাপী যোগাযোগ মাধ্যম। এটি ব্যাংক এবং আর্থিক প্রতিষ্ঠানের মালিকানাধীন এবং তারাই এটি ব্যবহার করে। নেটওয়ার্কটিতে SAP নামে কিছু অ্যাক্সেস পয়েন্ট রয়েছে, যার মাধ্যমে ব্যবহারকারীরা সুইফট নেটওয়ার্কে প্রবেশ করে। বাংলাদেশের কাছাকাছি দুটি SAP সিঙ্গাপুর এবং ভারতের মুম্বাইতে অবস্থিত। বাংলাদেশের সদস্য ব্যাংকগুলো নেটওয়ার্কে বার্তা জমা দেওয়া এবং গ্রহণ করার জন্য সিঙ্গাপুরে ISD টেলিফোন কল করে।

ব্যাংকগুলোকে কম্পিউটার, ইউপিএস, প্রিন্টার, লিজড-লাইন সাপোর্ট মডেম, Eicon কার্ড, উইন্ডোজ এনটি বা ইউনিক্স সফ্টওয়্যার ক্রয় করতে হয়। ঐসবের পরিমাণ নির্ভর করবে ব্যাংকগুলোর দ্বারা নির্বাচিত সুইফট এ্যালায়েন্স সফ্টওয়্যারের ধরনের ওপর। অ্যালায়েন্স সফ্টওয়্যার দুটি ধরনের রয়েছে অ্যালায়েন্স এন্ট্রি এবং অ্যালায়েন্স অ্যাক্সেস। 'অ্যালায়েন্স এন্ট্রি' একটি স্বতন্ত্র সফ্টওয়্যার এবং এর জন্য এক সেট হার্ডওয়্যার এবং উইন্ডোজ এনটি প্রয়োজন। 'অ্যালায়েন্স অ্যাক্সেস' হলো একটি মাল্টি-প্ল্যাটফর্ম, বহু-ব্যবহারকারী সফ্টওয়্যার। বার্তার সংখ্যা, শাখার সংখ্যা ও সফটওয়্যারের ধরনের ওপর নির্ভর করে একাধিক সেট হার্ডওয়্যারের প্রয়োজন হতে পারে। অ্যালায়েন্স অ্যাক্সেস সফ্টওয়্যার একটি ল্যান (লোকাল এরিয়া নেটওয়ার্ক) টার্মিনাল বা ডায়াল-আপ/লিজ-লাইন এবং মডেম দ্বারা সংযুক্ত দূরবর্তী শাখাগুলোতে অবস্থিত কম্পিউটারগুলো থেকে সুইফট অপারেশন করার সুযোগ দেয়। যদি লিজড-লাইন ব্যবহার করা হয় এবং শাখাগুলোর মধ্যে WAN স্থাপন করা হয়, তাহলে বার্তাগুলো স্বয়ংক্রিয়ভাবে শাখাগুলোতে রুট করা যায়। ইনওয়ার্ড বার্তাগুলো প্রথমে হেড অফিসে পৌঁছাবে এবং তারপর সংশ্লিষ্ট শাখাগুলোতে বিতরণ করা হবে। আউটওয়ার্ড বার্তাগুলো সংশ্লিষ্ট শাখাগুলো থেকে প্রথমে হেড অফিসের সার্ভারে আসে, তারপর সেগুলো SAP-তে পাঠানো হয়। অ্যালায়েন্স অ্যাক্সেস সফ্টওয়্যার এছাড়াও ফ্যাক্স এবং টেলেক্স থেকে বার্তা পাঠাতে/গ্রহণ করতে পারে।

অ্যালায়েন্স এন্ট্রি ও অ্যালায়েন্স অ্যাক্সেস সফটওয়্যার দুটিই ব্যাংকিং অ্যাপ্লিকেশন সফ্টওয়্যার থেকে ইনপুট গ্রহণ করতে পারে। যদি ব্যাংকিং সফ্টওয়্যারটি সুইফট ফরম্যাটে আউটওয়ার্ড বার্তা তৈরি করতে এবং ইনওয়ার্ড বার্তাগুলো পড়তে এবং প্রক্রিয়া করতে সক্ষম হয়, তাহলে কোনো সুইফট অপারেটরের প্রয়োজন নেই। এই পদ্ধতিতে ডুপ্লিকেট তথ্য পোস্ট করা বন্ধ করতে সক্ষম, যা প্রথম বার ব্যাংকিং অ্যাপ্লিকেশন সফ্টওয়্যারে এবং দ্বিতীয়বার সুইফট সফ্টওয়্যারে সংঘটিত হয়।

তবে বর্তমানে প্রায় সকল ব্যাংকই আলোচ্য সংযোগ পদ্ধতির পাশাপাশি ইন্টারনেট ব্যবহার করে সুইফটে সংযোগ স্থাপন করছে।

### ১২.২.৭. সুইফটের সমস্যাগুলো কী?

সুইফটের কিছু অসুবিধা রয়েছে। এর এককালীন ব্যয় এবং বার্ষিক সহায়তা চার্জ বেশি। একটি ব্যাংকের জন্য এককালীন সদস্যপদ চার্জটি প্রায় ২৫ লাখ টাকা এবং বার্ষিক সহায়তা চার্জটি প্রায় ৪.৫ লাখ টাকার কাছাকাছি। ব্যাংকগুলোর কম্পিউটার ও পেরিফেরিয়ালগুলোতেও বিনিয়োগের প্রয়োজন হবে। বাংলাদেশের ব্যাংকগুলোর জন্য, SAP সিঙ্গাপুরে অবস্থিত সুতরাং বার্তা সংগ্রহ ও সংক্রমণের জন্য ব্যাংকগুলোকে সিঙ্গাপুরে আইএসডি টেলিফোন কল করতে হবে। যদি সুইফট, ঢাকায় তার SAP ইনস্টল কওে, তবে এই ব্যয় হ্রাস করা যেতে পারে। আরেকটি উপায় হলো ব্যাংকগুলোকে সুইফট নেটওয়ার্কগুলোকে সংযোগের জন্য বিটিটিবির X.25 পিএসডিএন (পাবলিক সুইচ ডেটা নেটওয়ার্ক) ব্যবহার করার অনুমতি দেওয়া। তবে সুরক্ষার কারণে সুইফট বিটিটিবির X.25 নেটওয়ার্কের সঙ্গে সংযোগ সরবরাহ করতে সম্মত হয় না। সুইফ্টের SITA এর X.25 নেটওয়ার্কের সঙ্গে সংযোগ রয়েছে (যা এয়ারলাইন টিকিট সিস্টেমের জন্য বিশ্বব্যাপী ব্যবহৃত হচ্ছে)। যদি ব্যাংকগুলো SITA থেকে সংযোগের ব্যবস্থা করতে পারে তবে সুইফট হয়তো ব্যাংকগুলোকে এই সংযোগটি ব্যবহার করে সিঙ্গাপুরে SAP এর সঙ্গে সংযোগ স্থাপনের অনুমতি দিতে পারে। তবে বর্তমানে ব্যাংকগুলো ইন্টারনেট ব্যবহার করে সুইফটের সঙ্গে সংযুক্ত হচ্ছে, যা মোটেই ব্যয়বহুল নয়।

### ১২.২.৮. বাংলাদেশে ব্যবহারকারী গ্রুপ

প্রথম প্রজন্মের ব্যাংকগুলো : বাংলাদেশের সাতটি বেসরকারি খাতের ব্যাংক ১৯৯৯ সালে সুইফটের প্রথম প্রজন্মের সদস্য হয়েছিল। ব্যাংকগুলো হলো বেসিক, প্রাইম ব্যাংক, এবি ব্যাংক, ইসলামী ব্যাংক, আইএফআইসি, ইউসিবিএল এবং এনসিসি ব্যাংক।

দ্বিতীয় প্রজন্মের ব্যাংক (২০০০ সালের জুনে কাটওভার) : বাংলাদেশের তিনটি বেসরকারি খাতের ব্যাংক সুইফটের ২য় প্রজন্মের সদস্য। ব্যাংকগুলো হলো ডাচ্-বাংলা ব্যাংক, বাংলাদেশ ব্যাংক এবং ঢাকা ব্যাংক।

তৃতীয় প্রজন্মের ব্যাংকগুলো (আজ অবধি কাটওভার) : বাকি ব্যাংকগুলো সুইফটের তৃতীয় প্রজন্মের সদস্য।

সমস্ত দেশে, যেখানে আর্থিক ইনস্টিটিউটগুলো সুইফট ব্যবহার করছে, সেখানে কয়েকটি ব্যবহারকারী গ্রুপ এবং একটি ন্যাশনাল গ্রুপ রয়েছে।

বাংলাদেশে, প্রথম প্রজন্মের অংশগ্রহণকারী সব ব্যাংক নিয়ে প্রথম ব্যবহারকারী গ্রুপ গঠিত হয়েছিল। এই ব্যবহারকারী গ্রুপটি ন্যাশনাল গ্রুপের প্রতিনিধিত্ব করে।

### ১৩.৩. বাংলাদেশ অটোমেটেড ক্লিয়ারিং হাউস (BACH)

ম্যানুয়াল চেক ক্লিয়ারিং স্বাধীনতার পরপরই বাংলাদেশ ব্যাংক দ্বারা প্রাথমিকভাবে

চালু করা হয়েছিল। তারপরে বাংলাদেশ ব্যাংকের পক্ষে সোনালী ব্যাংকের দ্বারা পরিচালিত ৩১টি জেলায় আরও ৩৩টি ক্লিয়ারিং হাউস প্রসারিত করা হয়েছিল।

ম্যানুয়াল ক্লিয়ারিংয়ের বেশ কিছু অসুবিধা রয়েছে যেমন—

—ইনস্ট্রুমেন্টের বাস্তব চলাচলের প্রয়োজন।

—একই ক্লিয়ারিং হাউসের মধ্যেও ক্লিয়ারিং এর জন্য বেশ কয়েক দিনের জন্য প্রয়োজন হতো।

—আন্তঃক্লিয়ারিং হাউজগুলোর মধ্যে ক্লিয়ারিংয়ের জন্য OBC-এর প্রয়োজন হতো যা প্রক্রিয়া করতে ১ থেকে ৩ সপ্তাহ সময় নিত।

—অনেক ম্যানুয়াল প্রক্রিয়া এবং কাজের ডুপলিকেশন।

—দুর্বল এমআইএস।

উপরোক্ত বিষয়গুলো কাটিয়ে উঠতে বাংলাদেশ ব্যাংক ২০০৬ সালে বাংলাদেশ অটোমেটেড ক্লিয়ারিং হাউস (BACH) বাস্তবায়নের জন্য একটি প্রকল্প গ্রহণ করেছিল।

BACH-এর দুটি উপাদান রয়েছে

- BACPS— ব্যাংলাদেশ স্বয়ংক্রিয় চেক প্রসেসিং সিস্টেম এবং
- BEFTN— বাংলাদেশ ইলেকট্রনিক তহবিল স্থানান্তর নেটওয়ার্ক

### ১২.৩.১. বাংলাদেশ অটোমেটেড চেক প্রসেসিং সিস্টেম (BACPS)

BACPS বাংলাদেশ ব্যাংকের BACH প্রকল্পের একটি উপাদান। BACPS ২০১১ সালের অক্টোবরে বাংলাদেশ ব্যাংক ক্লিয়ারিং হাউসে সংযুক্ত হয়েছে।

BACPS-এর সুবিধাসমূহ

- যেহেতু ইন্সট্রুম্যান্ট ভ্রমণ করে না, তাই এটি দ্রুত কাজ করে।
- এটি একটি কেন্দ্রীয় সমাধান ফলে যে কোনো অঞ্চলের ইন্সট্রুম্যান্ট একদিনেই ক্লিয়ারিং করা যায়।
- সমস্ত অঞ্চলের জন্য হাই-ভ্যালু ক্লিয়ারিং চালু করা সম্ভব হয়েছে।
- উচ্চ দক্ষতা, কম ব্যয়।
- উচ্চতর গ্রাহক সন্তুষ্টি।
- শক্তিশালী এমআইএস।

### ১২.৩.২. বাংলাদেশ ইলেক্ট্রনিক তহবিল স্থানান্তর নেটওয়ার্ক (BEFTN)

BEFTN ২০১১ সালের ফেব্রুয়ারিতে চালু হয়েছে। BEFTN ইলেক্ট্রনিক উপায়ে ব্যাংকগুলোর মধ্যে তহবিলের লেনদেনকে সহায়তা করে। এটি নিম্নলিখিত লেনদেনে সহায়তা করে—

- পে-রোল
- বিদেশি রেমিট্যান্স বিতরণ।
- ডমেস্টিক রেমিট্যান্স বিতরণ।
- কোম্পানির লভ্যাংশ বিতরণ।
- অবসর ভাতা প্রদান।
- কর্পোরেট পেমেন্ট প্রদান।
- সরকারি ভাতা প্রদান।

এটির দেশব্যাপী কভারেজ রয়েছে। সরকারের ১০০% মন্ত্রণালয় এবং বিভাগগুলো BEFTN ব্যবহার করে তাদের বেতন বিতরণ করছে। বিদেশি রেমিট্যান্সের একটি বড় অংশ BEFTN ব্যবহার করে বিতরণ করা হয়। যেমন কোনো বিদেশি রেমিট্যান্স ব্যাংক-A-তে এসেছে, কিন্তু এর সুবিধাভোগীর অ্যাকাউন্ট ব্যাংক-B-এর সঙ্গে রয়েছে, তখন ব্যাংক-A BEFTN ব্যবহার করে ব্যাংক-B-তে রেমিট্যান্স স্থানান্তর করে থাকে।

### ১২.৪. এনপিএসবি (NPSB)

ন্যাশনাল পেমেন্ট সুইচ, বাংলাদেশ (এনপিএসবি) আর্থিক লেনদেনের জন্য একটি ইলেকট্রনিক প্ল্যাটফর্ম। কার্ডভিত্তিক ও ইন্টারনেট ভিত্তিক আর্থিক লেনদেনের ক্ষেত্রে, এটি বাংলাদেশের ব্যাংকগুলোকে একে অপরের সঙ্গে সংযুক্ত করে। কার্ডভিত্তিক আর্থিক লেনদেনগুলো এটিএম এবং পস টার্মিনাল ব্যবহার করে শুরু করা হয়। ফলে ব্যাংক-A এর গ্রাহক অর্থ উত্তোলনের জন্য ব্যাংক-B এর এটিএম ব্যবহার করতে পারেন। ব্যাংক-A এর সঙ্গে তার অ্যাকাউন্টটি তাৎক্ষণিকভাবে বাংলাদেশ ব্যাংকের NPSB সিস্টেমের মাধ্যমে ডেবিট করা হবে। একইভাবে, ব্যাংক-A এর গ্রাহক ব্যাংক-B দ্বারা ইনস্টল করা একটি পস টার্মিনাল থেকে তার শপিং বিলগুলো প্রদান করতে পারেন। গ্রাহক কার্ডভিত্তিক আর্থিক লেনদেনের জন্য কোনো ডেবিট বা ক্রেডিট কার্ড ব্যবহার করতে পারেন।

ইন্টারনেটভিত্তিক আর্থিক লেনদেন তখনই হয় যখন গ্রাহক তার ব্যাংকের (ব্যাংক-A) ইন্টারনেট ব্যাংকিং সিস্টেমটি ব্যবহার করে ব্যাংক-B এর অন্য একজন গ্রাহকের অ্যাকাউন্টে অর্থ স্থানান্তর করতে চান। এক্ষেত্রে গ্রাহককে তার লেনদেনটি অনুমোদনের জন্য 2FA (টু-ফেক্টর অথেনটিকেশন) ব্যবহার করতে হয়।

### ১২.৫. আরটিজিএস (RTGS)

রিয়েল টাইম গ্রস সেটেলমেন্ট (আরটিজিএস) 'রিয়েল-টাইম'-এ একটি বড় অংকের তহবিল এক ব্যাংক থেকে অন্য ব্যাংকে স্থানান্তরের জন্য ব্যবহৃত হয়। এটি ব্যাংকিং চ্যানেলের মাধ্যমে দ্রুততম অর্থ স্থানান্তরের সিস্টেম। 'রিয়েল-টাইম'-এ নিষ্পত্তি মানে অর্থ প্রদানের লেনদেন তৎক্ষণাৎ সংঘঠিত হয়। 'গ্রস সেটেলমেন্ট' অর্থ লেনদেনটি অন্য কোনো লেনদেনের সঙ্গে সংযুক্ত বা নেট না করে একটি একটি করে নিষ্পত্তি করা হয়। যেহেতু কেন্দ্রীয় ব্যাংকের লেজারে অর্থ স্থানান্তর সংঘটিত হয়, তাই এই সিস্টেমে অর্থ প্রদান চূড়ান্ত এবং অপরিবর্তনীয় হিসাবে ধরে নেওয়া হয়।

### ১২.৬. চিপস (CHIPS)

৪০ বছরেরও বেশি সময় ধরে, চিপস (ক্লিয়ারিং হাউস ইন্টারব্যাংক পেমেন্টস সিস্টেম) ওয়্যার ট্রান্সফার প্রদানের ক্ষেত্রে নির্ভরযোগ্যতা, দক্ষতা এবং উদ্ভাবনের মাধ্যমে একটি ইন্ডাস্ট্রি স্ট্যান্ডার্ড নির্ধারণ করেছে। বিশ্বব্যাপী শীর্ষস্থানীয় ব্যাংকগুলো, তাদের করোসপেন্ডেন্ট এবং গ্রাহকরা নির্ভুল ও রিয়েল-টাইম পেমেন্টের জন্য চিপসের ওপর নির্ভরশীল। বর্তমানে ইউএস ক্রস-বর্ডার লেনদেনের ৯৫% এবং আভ্যন্তরীণ লেনদেনের প্রায় অর্ধেক চিপসের মাধ্যমে সংঘটিত হয়, যা প্রাত্যহিক আয় ১.৫ ট্রিলিয়ন ডলারের সমান।

চিপস 'দ্য ক্লিয়ারিং হাউস' দ্বারা পরিচালিত হয়, যা বিভিন্ন ধরনের আর্থিক প্রতিষ্ঠানের জন্য ACH, পেপার চেক এক্সচেঞ্জ এবং চেক ইমেজ এক্সচেঞ্জ সার্ভিসও প্রদান করে থাকে।

### ১২.৭. ফেডওয়ার (FEDWIRE)

আনুষ্ঠানিকভাবে ফেডারেল রিজার্ভ ওয়্যার নেটওয়ার্ক হিসাবে পরিচিত, ফেডওয়ার হলো ফেডারেল রিজার্ভ ব্যাংকগুলো দ্বারা পরিচালিত একটি রিয়েল টাইম গ্রস সেটেলমেন্ট ফান্ড ট্রান্সফার সিস্টেম, যা আর্থিক প্রতিষ্ঠানগুলো ইলেকট্রনিকভাবে তার ৯,২৮৯ এরও বেশি সদস্যের (মার্চ ১৯, ২০০৯ পর্যন্ত) মধ্যে তহবিল স্থানান্তর করতে পারে। বেসরকারিভাবে অনুষ্ঠিত ক্লিয়ারিং হাউস ইন্টারব্যাংক পেমেন্টস সিস্টেম (CHIPS) এর সঙ্গে একত্রে FEDWIRE একটি হাই-ভ্যালু ও টাইম-ক্রিটিকাল দেশীয় এবং আন্তর্জাতিক অর্থ প্রদানের জন্য মার্কিন যুক্তরাষ্ট্রের একটি প্রধান নেটওয়ার্ক। এটি অত্যন্ত স্থিতিস্থাপক (resilient) এবং রিডান্ডেন্ট হওয়ার

জন্য ডিজাইন করা হয়েছে। ২০০৭ সালে ফেডওয়ারের মাধ্যমে স্থানান্তরিত মুদ্রার গড় ছিল দৈনিক প্রায় ২.৭ ট্রিলিয়ন ডলার এবং দৈনিক গড় অর্থ প্রদানের সংখ্যা ছিল প্রায় ৫৩৭,০০০টি।

## পর্যালোচনামূলক প্রশ্নাবলি

**1) Multiple Choice Questions (MCQ)**

i) Which one is not an Alternative Delivery Channel?

a) ATM b) Branch c) Agent Banking d) Internet Banking

ii) In which device, cash can be deposited by the customer?

a) ATM b) POS c) CRM d) UPS

iii) Which protocol is used in ATM to communicate with a Switch?

a) TCP/IP b) LAN c) NDC+ d) C++

iv) Which bandwidth is required for ATM communication?

a) 64 kbps b) 1 Gbps c) 16 kbps d) 512 kbps

v) Why a card become a hot card and thus captured by ATM?

a) Insufficient cash in ATM b) Insufficient balance in account c) Wrong PIN used 3 times d) Wrong amount inserted 3 times

vi) Which of the following is a card fraud?

a) Skimming b) Clustering c) Replication

d) Encryption

vii) Which of the following is not a POS transaction?

a) Sale b) Void c) Refund d) Buy

viii) Pre-authorization transaction in POS is usually used in which merchant?

a) Electronic b) e-commerce c) Hotel d) Grocery

ix) The printer used in a POS terminal is called:

a) Dot Matrix b) Laser Jet c) Vacuum d) Thermal

x) The Bank which issue a credit card is called:

a) Issuer b) Acquirer c) Merchant d) Branch

xi) Off-us transactions are also called:

a) Not on-us b) Remote on-us c) Remote off-us d) None of the above

xii) Which one is not a debit card income?

a) Issuance fee b) Renewal fee c) Replacement fee d) Late payment fee

xiii) Internet Banking is also known as:

a) Online banking b) Branch banking c) Smart banking d) Home banking

xiv) Which of the following is not a P2B transaction?

a) Utility Bills Payment b) Mobile TopUp c) Merchant Payment d) Income Tax Payment

xv) Which of the following is not a category of Swift customer?

a) Member b) Sub-member c) Participants d) Principal member

**2. Fill in the gap(s)**

i) In case of cash non-dispensed from ATM, the cardholder should report to …

ii) Bangladesh Bank is the …generation member of use groups of SWIFT in Bangladesh.

iii) BACH has two components: a) …and b) …

iv) BEFTN went live on …

v) There are two types of ATMs: Lobby Type and …type.

vi) EMV stands for ….

vii) ATM safe is available in two standards: UL and ….

viii) The captured cash of ATM is stored in ….

ix) POS stands for ….

x) A POS terminal can communicate with Data Center using PSTN or….

xi) Recording of information on the magnetic strip is called ….

xii) In the EMVCo … MasterCard and VISA each have 25% share.

xiii) Phishing is collection of …by presenting a fake web-site address to the user.

xiv) Buying and selling of goods and services over internet is called…

xv) SWIFT stands for ….

xvi) BEFTN stands for ….

xv) RTGS stands for …

# সম্ভাব্য প্রশ্নাবলি

1. Name 10 channels for alternative delivery of banking services and 7 fund transfer systems.
2. List 5 components of an ATM.
3. What is the function of a cash dispenser in ATM?
4. What services a customer gets from an ATM?
5. How ATM works in case of on-us debit card transaction and on-us credit card transaction?
6. How ATM works in case of not-on-us transaction using an international credit card?
7. Mention the differences between a lobby type and the through-the-wall type ATM.
8. Mention the function of a card reader in ATM.
9. Why a printer is required in ATM?
10. Which technology is used for counting and dispensing money from ATM?
11. Which safe is stronger – UL291 or CEN? Why?
12. Why number of times cash is refilled in CRM is lower than that in ATM?
13. How bank resolve the issue of cash non-dispensed, but account is credited?
14. What is a reject bin and why it is used?
15. What kind of connectivity is use in ATM?
16. What is hot card?
17. List the different expense heads of an ATM booth.
18. How skimming happen and how this can be stopped?
19. ATM + CDM = CRM. Explain.
20. How a POS terminal is used for settlement of merchant bill?
21. How a POS terminal id connected to server in datacenter?
22. Describe following functions of a POS terminals: Sale, Void, Refund, Pre-auth, Cash Advance.
23. Describe how a not-on-us transaction occurs in a POS terminal.
24. Describe the following : PIN Pad, Merchant Commission, Interchange fee.
25. Narrate the different types of frauds found in POS terminal and their remedies.
26. What are the different type of cards? Describe any two of them.
27. Define the following in relation to cards : Issuer, Acquirer, On-Us transaction, Not-on-us transaction, Remote on-us transaction, Charge back.
28. What are the differences between an EMV card and Chip card?
29. What is Liability Shifting?
30. Name five international payment associations. Write a paragraph on any one of them.
31. What are the source of income of a bank from credit card business?
32. What do you mean by card personalization?
33. Define card encoding and card embossing.
34. Write a paragraph on card fraud and its prevention.
35. What are the technological solutions against card counterfeiting?
36. What is EMV? How it is secured?
37. Why banks should move to EMV?

38. What are the standard rules to follow by Internet Banking clients?
39. Mention 3 valid and 3 invalid password for Internet Banking.
40. List a few functions of an Internet Banking.
41. What are the common frauds in Internet Banking and how these can be prevented?
42. How phishing is used in collecting Internet Banking log-in ID and Password?
43. What is a digital signature? Where and why it is used?
44. What is a two-factor-authentication? How this prevent Internet Banking fraud?
45. Mention a few differences between sms and alert banking.
46. Sate the life cycle of an e-commerce transaction?
47. How Internet Payment Gateway works?
48. How an OTP can secure an e-commerce transaction?
49. What are the common frauds in e-commerce transaction and what are the possible remedies?
50. Mention five MFS activities. Describe any two of them.
51. Why transaction limit is imposed in MFS?
52. Why MFS is not cheap for customers?
53. What are the differences among Bank-led, Non-Bank-Led and Bank-NBFI-Govt-Lead MFS models? Currently which model is prevailing in our country?
54. Describe advantages and disadvantages of using sms and USSD as connectivity media for MFS.
55. What is an Agent Banking? What are the objectives of introduction of Agent Banking in Bangladesh?
56. Write a para on the history of Agent Banking.
57. What is the strategy behind introduction of Agent Banking in Bangladesh?
58. Write the resent status of Agent Banking in Bangladesh with respect to Number of Outlets, accounts, banks in Agent banking, and amount of deposit, Credit and inward foreign remittance.
59. Describe Distribution-Led model of Agent Banking.
60. Differentiate between the models : Unit agemt model and bank led model.
61. What are differences among : Agent, Sub-Agent and Unit Agent?
62. What kind of banking services are allowed in Agent Banking?
63. Which banking services are not allowed in Agent Banking?
64. What are the current transaction limits for Savings account holders in Agent Banking?
65. When an Agent Banking become profitable?
66. Mention a few of the challenges of Agent Banking.
67. What is a Call Center?
68. What are the differences between a Call Center and a Contact Center?
69. Name the different modes of communication for a Contact Center?
70. What are the key components of a Contact Center? Narrate them.
71. Present Call Flows of a Call Center.
72. Write key features of self-service and assisted-service of a all Center?
73. List five common Inbound and five common outbound activities of a Call Center.
74. What do you mean by Quality Assurance at a Call Center?

75. What is the abbreviation of SWIFT?
76. What are the three different categories of membership in SWIFT? Narrate two of them.
77. Why a bank should become a member of SWIFT?
78. Is the SWIFT secured? Why?
79. How SWIFT works?
80. What are the drawbacks of SWIFT?
81. What are the abbreviations of the followings:
    a) BACH, b) BACPS, c) BEFTN, d) NPSB, e) RTGS
82. What are the demerits of manual clearing house? What was the solution to these issues?
83. What are the benefits of BACPS?
84. What transactions can be performed using BEFTN?

মডিউল-ডি

# আইসিটি নিরাপত্তা, সাইবার নিরাপত্তা, আইসিটি ঝুঁকি ব্যবস্থাপনা, মান, প্রবিধান ও আইনি কাঠামো

**১. আইসিটি নিরাপত্তা (ICT Security)**

আইসিটি সিকিউরিটি হলো একটি নিরাপত্তা ব্যবস্থা, যা অভ্যন্তরীণ ও বাহ্যিক হুমকি থেকে একটি প্রতিষ্ঠানের আইটি অবকাঠামো, নেটওয়ার্ক, ডেটা এবং তথ্য সুরক্ষিত করতে ব্যবহৃত হয়। এর মধ্যে রয়েছে ফিজিক্যাল সিকিউরিটি, নেটওয়ার্ক সিকিউরিটি, ডেটা সেন্টার এবং ডিআরএস সিকিউরিটি, এক্সেস কন্ট্রোল, ভাইরাস প্রোটেকশন, ডাটাবেস সিস্টেম সিকিউরিটি, ইমেল সিকিউরিটি এবং এডিসি এবং ব্যাংক কার্ড এর নিরাপত্তা।

১৯৮০ সালে বাংলাদেশে ব্যাংকিং কার্যক্রমের কোনো অটোমেশন ছিল না। গ্রাহকদের অ্যাকাউন্টের ব্যালেন্স এবং ডেবিট ও ক্রেডিটের মতো লেনদেন রেকর্ড করতে একটি বড় ম্যানুয়াল লেজার ব্যবহার করা হতো। অ্যাকাউন্টের সুদের পরিমাণ একটি ক্যালকুলেটর ব্যবহার করে গণনা করা হতো যার ফলাফল একটি বড় ফিজিক্যাল লেজারে রেকর্ড করা হতো। ইন্টারনেট, সাইবার সিকিউরিটি, হ্যাকিং, ফিশিং, র‍্যানসমওয়্যার, ম্যালওয়্যার, ভাইরাস, অ্যান্টিভাইরাস, ফায়ারওয়াল, রাউটারের মতো কয়েকটি শব্দের অস্তিত্ব তখন ছিল না।

ধীরে ধীরে, ব্যাংকগুলো প্রতিটি মাসের শেষে অ্যাকাউন্ট ব্যালেন্স, এর লেনদেন এবং বকেয়া সুদের হিসাব রেকর্ড করতে সফ্টওয়্যার চালু করতে শুরু করে। ফলে একজন ব্যাংকারের ডিউটি উল্লেখযোগ্যভাবে হ্রাস পেয়ে যায় এবং ব্যাংকাররা তাতে অনেকাংশে খুশি হয়। এই অ্যাকাউন্ট ব্যালেন্স এবং লেনদেনগুলো একটি কম্পিউটারের স্থানীয় হার্ড ডিস্কে রেকর্ড করা হতো। একই ব্যাংকের অন্য শাখার সঙ্গে সংযোগের প্রয়োজন ছিল না।

পরবর্তীতে, অন্যান্য ব্যাংকিং কার্যক্রম যেমন জেনারেল লেজার, ক্রেডিট সংক্রান্ত কার্যাবলি এবং বৈদেশিক বাণিজ্য সংক্রান্ত কার্যাবিল সফ্টওয়্যারটিতে যুক্ত করা হয়, যা ব্যাংকারদের আরও বেশি স্বস্তি দিয়েছে।

অবশেষে, বিভিন্ন ক্লায়েন্টদের কাছ থেকে আন্তঃ-শাখা লেনদেন এবং এটিএম থেকে টাকা উত্তোলনের দাবি, ব্যাংকগুলোকে একটি সেন্ট্রালাইজড সফ্টওয়্যার স্থাপন করতে বাধ্য করে। ফলে অ্যাকাউন্টের ব্যালেন্স এবং অ্যাকাউন্টের সমস্ত লেনদেন কেন্দ্রীয়ভাবে একটি ডেটা সেন্টারে রেকর্ড করা হয়। এতে সারা দেশে

ব্যাংকের ডেটাবেস উন্মোচিত হয়। সারা দেশে অবস্থিত শাখা এবং এটিএমগুলো একটি ওয়াইড এরিয়া নেটওয়ার্ক (ওয়ান) ব্যবহার করে কেন্দ্রীয় ডেটাবেস অ্যাক্সেস করে। ডেটাবেসে অননুমোদিত অ্যাক্সেস এবং গ্রাহকের ডেটা চুরির ঝুঁকি (এবং যেমন অর্থ) প্রথমবারের জন্য উদ্বেগের বিষয় হয়ে ওঠে। আইটি পেশাদাররা তাদের ডাটাবেস রক্ষা করতে শুরু করে এবং নেটওয়ার্কে ফায়ারওয়াল স্থাপন করে।

তারপরে বাড়ি, অফিস বা দেশের বাইরে থেকে গ্রাহকদের অ্যাকাউন্ট অ্যাক্সেস করার দাবি একটি গুরুত্বপূর্ণ বিষয় হয়ে ওঠে এবং ভিসা ও মাস্টারকার্ড ক্রেডিট কার্ড লেনদেনের জন্য দেশের বাইরে যোগাযোগের প্রয়োজনে ব্যাংকগুলোকে ইন্টারনেটের সঙ্গে সংযোগ করতে বাধ্য করে। ইন্টারনেটের সঙ্গে ব্যাংকের সংযোগ পুরো ব্যাংকিং ব্যবস্থাকে নিরাপত্তার জন্য খুবই ঝুঁকিপূর্ণ করে তোলে। ফলস্বরূপ, দেশের বা বিশ্বের যে কোনো জায়গা থেকে হ্যাকাররা ব্যাংকের নেটওয়ার্কিং সিস্টেমে কোনো সুরক্ষা ত্রুটি খুঁজে পেলে তারা অতি সহজেই ব্যাংকিং ডেটাবেসে অ্যাক্সেস পেতে পারে।

এই পর্যায়ে, ডেটা সেন্টার (ডিসি) একটি ব্যাংকের আইটি সিস্টেমের সবচেয়ে গুরুত্বপূর্ণ অংশ হয়ে উঠেছে। যেকোনো দুর্যোগের ক্ষেত্রে ডেটা নিরাপদ এবং সহজলভ্য রাখতে, আইটি পেশাদাররা একটি ডিজাস্টার রিকভারি সাইট (ডিআরএস) এবং নিয়ার ডেটা সেন্টার (এনডিসি) তৈরি করেন। প্রাকৃতিক দুর্যোগের ক্ষেত্রে ডেটা পুনরুদ্ধারের জন্য ডিআরএস একটি ভিন্ন সিসমিক জোনে তৈরি করা হলেও, ডিসিতে বড় বা ছোটখাটো দুর্ঘটনার ক্ষেত্রে দ্রুত অপারেশন শুরু করার জন্য একই শহরে এনডিসি তৈরি করা হয়।

যেহেতু বাংলাদেশের ব্যাংকগুলোতে সমস্ত প্রযুক্তিগত উদ্ভাবন রয়েছে, তাই আইসিটি হুমকিগুলোকে নিম্নরূপভাবে বিভক্ত করা যেতে পারে—

### ১.১. ব্যবসার ধারাবাহিকতা হুমকি (Business Continuty Threats)

এটি এক ধরনের হুমকি যার ফলে ডেটা সেন্টারে কোনো সার্ভার বা সরঞ্জামের ফেইলিউর ঘটে এবং সিস্টেমটি ব্যবহারকারী এবং গ্রাহকদের কাছে অনুপলব্ধ (unavailable) থাকে। শাখার কর্মকর্তারা গ্রাহকদের ব্যাংকিং সেবা প্রদান করতে পারেন না। এছাড়াও গ্রাহকরা এটিএম, পিওএস, ই-কমার্স সাইট বা ইন্টারনেট ব্যাংকিংয়ে লেনদেন করতে পারেন না। গ্রাহকরা অসন্তুষ্ট হন এবং ব্যাংক ব্যবসার ধারাবাহিকতা নিশ্চিত করতে না পারলে তারা ব্যাংক ছেড়ে যেতে পারেন। ব্যবসায় বিরতি নিম্নরূপভাবে শ্রেণিবদ্ধ করা যেতে পারে—

**ক) সরল ব্রেকডাউন (Simple Breakdown)**

ডেটা সেন্টারে সহজ বা সামান্য ব্রেকডাউনের কারণে, সিস্টেম কয়েক মিনিট থেকে কয়েক ঘণ্টার জন্য অনুপলব্ধ (unavailable) থাকতে পারে। এই ধরনের ভাঙনের কারণ এবং এর প্রতিকার টেবিল-১ এ দেওয়া আছে।

টেবিল ১

| কারণসমূহ | প্রতিকার |
|---|---|
| সার্ভার অ-কার্যকর | • ডেটাবেস সার্ভারের জন্য অ্যাক্টিভ-অ্যাক্টিভ ক্লাস্টারিংয়ের ব্যবহার<br>• অ্যাপ্লিকেশন সার্ভারের জন্য নেটওয়ার্ক লোড ব্যালেন্সিং (NLB) ব্যবহার করা |
| নেটওয়ার্ক সরঞ্জাম | রিডান্ডেন্ট অ্যাক্টিভ-অ্যাক্টিভ নেটওয়ার্ক ইকুইপমেন্ট ব্যবহার করা |
| ইউপিএস | রিডান্ডেন্ট ইউপিএস ব্যবহার |
| শীতলকরণ ব্যবস্থা | একটিভ-স্ট্যান্ডবাই কোলিং সিস্টেম ব্যবহার |

**খ) মেজর শাটডাউন (Major Shutdown)**

ডেটা সেন্টারে একটি বড় ব্রেকডাউনের কারণে, সিস্টেমটি কয়েক ঘণ্টা বা কয়েক সপ্তাহের জন্য অনুপলব্ধ থাকতে পারে। এই ধরনের ব্রেকডাউনের কারণ এবং এর প্রতিকার সারণি ২ এ দেওয়া হয়েছে।

টেবিল ২

| কারণসমূহ | প্রতিকার |
|---|---|
| ডেটাবেস (ডিবি) নষ্ট হয়ে যাওয়া | নিয়ার ডেটা সেন্টার স্থাপন করা<br>ডেটাবেজ নষ্ট হওয়ার পূর্বের অবস্থায় ফিরে যাওয়ার সুবিধা থাকা |
| স্টোরেজ নষ্ট হয়ে যাওয়া | নিয়ার ডেটা সেন্টার স্থাপন<br>একই ডিসি বা নিয়ার ডিসির আলাদা স্টোরেজে RMAN ব্যাকআপ নেওয়া |
| ডেটাসেন্টার আগুনে ক্ষতিগ্রস্ত হওয়া | নিয়ার ডেটা সেন্টার স্থাপন |

**গ) ভূমিকম্প, বন্যা ও ঘূর্ণিঝড়ের মতো প্রাকৃতিক দুর্যোগের কারণে ডেটা সেন্টার নষ্ট হয়ে গেলে (Data Center Collapsed due to natural calamity like Earthquake, Flood and Cyclone)**

ভূমিকম্প, বন্যা এবং ঘূর্ণিঝড়ের মতো প্রাকৃতিক দুর্যোগের কারণে ডেটা সেন্টারটি নষ্ট হয়ে পড়লে, সিস্টেমটি এক সপ্তাহ থেকে কয়েক মাস পর্যন্ত অনুপলব্ধ থাকতে পারে। এই ধরনের ক্ষেত্রে, ব্যবসা চালিয়ে যাওয়ার জন্য একটি ভিন্ন সিসমিক জোনে একটি ডিজাস্টার রিকভার সাইট বা বিপর্যয় মোকাবিলা কেন্দ্র বা (ডিআরএস) এবং একই শহরে একটি নিয়ার ডেটা সেন্টার (এনডিসি) তৈরি করা জরুরী। নিয়ার ডেটা সেন্টারটিতে ডেটা সেন্টারের মতো একই ক্ষমতা সম্পন্ন ইকুইপমেন্ট থাকতে হবে এবং একই ধরনের যোগাযোগ সংযোগ থাকতে হবে।

### ১.২. অভ্যন্তরীণ হুমকি (Internal Threats)

**ক) অসন্তুষ্ট বা দুর্নীতিগ্রস্ত কর্মচারী (Unsatisfied or Corrupt Employee)**
একটি ব্যাংকের অসন্তুষ্ট কর্মচারী বা দুর্নীতিগ্রস্ত কর্মচারীরা ডেটা বা তথ্য চুরি করে হ্যাকারদের হাতে তুলে দিতে পারে।

**খ) ডাটাবেস ব্রিচিং (Database Breaching)**
যদি একটি ডেটাবেস, যা সংবেদনশীল ব্যাংকিং বা ক্রেডিট কার্ড ডেটা সংরক্ষন করে, তা যদি ব্যাংকের অনেক অ্যাডমিনিস্ট্রেটরের কাছে সহজেই অ্যাক্সেসযোগ্য (একই পাসওয়ার্ড ভাগ করে) হয়, এটি ডেটা চুরি বা ইচ্ছাকৃতভাবে ডেটা ক্ষতির কারন হতে পারে। এমতাবস্থায় এর জন্য দায়ী অ্যাডমিনিস্ট্রেটরকে চিহ্নিত করা কঠিন।

### ১.৩. মোবাইল ফিন্যান্সিয়াল সার্ভিস (এমএফএস) সম্পর্কিত ঝুঁকি (MFS related Risks)

ওপরে বর্ণিত হুমকির কারণে মোবাইল ফাইন্যান্সিয়াল সার্ভিসেরও সেবার অনুপলব্ধতার ঝুঁকি রয়েছে। তবে এটি গ্রাহক ও দেশের জন্য নতুন ধরনের অন্যান্য ঝুঁকি নিয়ে এসেছে। এগুলো সারণি ৩ এ উপস্থাপন করা হয়েছে।

টেবিল-৩

| গ্রাহক বা দেশের জন্য ঝুঁকি | প্রতিকার |
|---|---|
| সিম ক্লোনিং ও MFS গ্রাহকের অ্যাকাউন্ট থেকে টাকা উত্তোলন | যখন একটি MNO খুচরা বিক্রেতার কাছে একটি আসল সিম অন্য একটি নতুন সিম দ্বারা প্রতিস্থাপিত হয়, তখন MNO এই তথ্যটি এমএফএস সেবা প্রদানকারী প্রতিষ্ঠানকে পাঠাবে। MFS সেবা প্রদানকারী প্রতিষ্ঠান অবিলম্বে গ্রাহকের অ্যাকাউন্ট ব্লক করবে। তারপর, MFS সেবা প্রদানকারী প্রতিষ্ঠান প্রকৃত সিম ধারকের কাছ থেকে একটি কল পাওয়ার পরেই যথাযথ যাচাইপূর্বক অ্যাকাউন্টটি পুনরায় সচল করবে। এতে সিম ক্লোনিং এর মাধ্যমে MFS অ্যাকাউন্টে প্রতারণা বন্ধ হয়ে যাবে। |
| চাঁদাবাজি / ব্ল্যাকমেইলিং / প্রতারণা / MFS গ্রাহকদের বোকা বানানো | চাঁদাবাজি ইত্যাদির মাধ্যমে, MFS গ্রাহকের অ্যাকাউন্ট থেকে অর্থ অন্য অ্যাকাউন্টে স্থানান্তর করা হয় (যার KYC মিথ্যা)। পরে যদিও গন্তব্য অ্যাকাউন্ট শনাক্ত করা যায় কিন্তু ঐ অ্যাকাউন্টের মালিক অজ্ঞাত রয়ে যায়। এটি নিম্নলিখিত উপায়ে হ্রাস করা যেতে পারে :<br>এমএফএস অ্যাকাউন্ট সক্রিয় করার আগে NID যথাযথভাবে যাচাইকরণ<br>সঠিকভাবে KYC ফরম পূরণ করা।<br>এছাড়াও একটি সচেতনতা প্রচারাভিযান গ্রাহকদের প্রতারিত না হতে ও শিক্ষিত করতে সাহায্য করতে পারে। |
| MFS ব্যবহার করে ঘুষ গ্রহণ, মানব পাচার ও মাদক বিক্রির জন্য অর্থ সংগ্রহ, সন্ত্রাসী অর্থায়ন | অবৈধ অর্থ সংগ্রহের জন্য এমএমএস অ্যাকাউন্ট ব্যবহার করা হতে পারে। অনেক ক্ষেত্রে ডেটাবেসে অবস্থিত অ্যাকাউন্ট খোলার ভুল তথ্যের কারণে এই ধরনের অ্যাকাউন্টের মালিক শনাক্ত করা যায় না। নিম্নলিখিত ব্যবস্থাগুলো দ্বারা এটি হ্রাস করা যেতে পারে :<br>এমএফএস অ্যাকাউন্ট সক্রিয় করার আগে এনআইডি যাচাইকরণ।<br>ওটিসি (ওভার দ্য কাউন্টার) লেনদেন কমানো।<br>সেংশন স্ক্রিনিং সিস্টেম এবং লেনদেন মনিটরিং সফটওয়্যার ব্যবহার করা। |
| MFS ব্যবহার করে ডিজিটাল হুন্ডি প্রেরণ এবং ফলস্বরূপ দেশ বৈদেশিক মুদ্রা থেকে বঞ্চিত হয় | ডিজিটাল হুন্ডি হলো এমএফএসের মাধ্যমে অবৈধভাবে বিদেশি রেমিট্যান্স প্রেরণ করছে। প্রচুর ডিজিটাল হুন্ডির কারণে, ২০১৭ সালে অভ্যন্তরীণ বিদেশি রেমিট্যান্সে ১৭% পতন রেকর্ড করা হয়েছিল। ডিজিটাল হুন্ডির পাশাপাশি ওপরে উল্লিখিত অন্যান্য অনিয়ম বন্ধ করার জন্য, এজেন্ট থেকে সরাসরি ক্যাশ |

| | |
|---|---|
| | আউট সীমা নূনতম পর্যায়ে কমিয়ে আনা যেতে পারে। প্রয়োজনে, যে কোনো ব্যাংকের সঙ্গে নিবন্ধিত ব্যাংক অ্যাকাউন্টের মাধ্যমে অতিরিক্ত ক্যাশ আউট করা যেতে পারে। এটি এমএফএসের সমস্ত অপব্যবহার বন্ধ করবে এবং একই সঙ্গে ওয়ালেটগুলোর ইলেকট্রনিক ব্যবহার বাড়িয়ে তুলবে। একটি 'সত্যিকারের ক্যাশলেস বাংলাদেশ' তৈরি করবে। |

## ১.৪. এটিএম/ পস/ ই-কম/ কার্ড সম্পর্কিত ঝুঁকি (ATM/POS/e-Com related Threats)

### ১.৪.১. এটিএম স্কিমিং (ATM Skimming)

স্কিমিং ধরনের ঝুকির কাছে এটিএম ও পস মোটেই নিরাপদ নয়। স্কিমাররা এটিএমের কার্ড স্লটে একটি ডিভাইস সংযুক্ত করে এবং কার্ডের তথ্য সংগ্রহ করে। এটিএম পিন রেকর্ড করতে একটি ক্যামেরা ব্যবহৃত হয়। তারপরে জালিয়াতরা সংগৃহীত তথ্য ব্যবহার করে একটি সদৃশ কার্ড (কার্ড ক্লোনিং নামে পরিচিত) তৈরি করে এবং কার্ড এবং পিন ব্যবহার করে এটিএম থেকে অর্থ উত্তোলন করে।

এটিএমে একটি অ্যান্টি-স্কিমিং ডিভাইস ব্যবহার করলে, তা স্কিমিং ডিভাইসে কার্ডের ডেটা অনুলিপি করতে বাধা দেয়। এই ধরনের অপরাধ দমন করার আরেকটি উপায় হলো গ্রাহকদের কাছে চিপ কার্ড ইস্যু করা। স্কিমিং ডিভাইসগুলো কোনও ডেবিট বা ক্রেডিট কার্ডের চিপ থেকে ডেটা কপি করতে পারে না।

### ১.৪.২. পস/পিওএস স্কিমিং (POS Skimming)

সুপার শপগুলোতে দুর্নীতিগ্রস্ত বিক্রয়কর্মীরা তাদের টেবিলের নিচে স্কিমিং ডিভাইসগুলো রাখে এবং গ্রাহকদের কার্ডগুলো প্রথমে স্কিমিং ডিভাইসে সুইপ করে. তারপর তারা টেবিলের ওপর রক্ষিত পিওএস টার্মিনালে এটি ব্যবহার করে। এভাবে তিনি কার্ডের তথ্য সংগ্রহ করেন, সংগৃহীত তথ্য ব্যবহার করে একটি কার্ড তৈরি করেন এবং সোনা বা ব্যয়বহুল ইলেকট্রনিক আইটেম কিনতে একটি পস টার্মিনালে তৈরি করা ক্লোন কার্ডটি ব্যবহার করেন।

এই ধরনের জালিয়াতি কেবল গ্রাহকদের চিপ কার্ড ইস্যু করে বন্ধ করা যেতে পারে। টেবিলের নিচে স্থাপন করা একটি স্কিমিং ডিভাইস কোনো ডেবিট বা ক্রেডিট কার্ডের চিপ থেকে ডেটা কপি করতে সক্ষম নয়।

### ১.৪.৩. এটিএম জ্যাকপটিং (ATM Jackpotting)

যদি হ্যাকাররা এটিএম কন্ট্রোলার (সুইচ নামে পরিচিত) এর নিয়ন্ত্রণ নিতে পারে তবে তারা এটিএম মেশিনে সংকেত প্রেরণ করতে পাওে, যা থেকে এটিএম বুঝতে পারে যে এখন তাকে অর্থ বিতরণ করতে হবে। এভাবে এটিএম কোনো কার্ড ছাড়াই অর্থ বিতরণ শুরু করে এবং হ্যাকারের সহযোগীরা নগদ অর্থ সংগ্রহ করে চলে যায়। একে এটিএম জ্যাকপোটিং বলে।

এটিএম কন্ট্রোলারকে এ জাতীয় ধরণের হ্যাকার থেকে রক্ষা করার জন্য, ব্যাংকের কম্পিউটার নেটওয়ার্কে অননুমোদিত অ্যাক্সেস রোধ করা প্রয়োজন।

### ১.৪.৪. ই-কমার্স জালিয়াতি (e-Commerce Fraud)

একটি ই-কমার্স সাইটে, কার্ডের নম্বর, মেয়াদোত্তীর্ণ তারিখ এবং একটি ৩-অক্ষরের গোপন নম্বর ব্যবহার করে কেনাকাটার বা সার্ভিসের বিল প্রদান করা যেতে পারে। এসব তথ্য একটি কার্ডের গায়ে লিখিত আছে।

যখন কোনো কার্ড রেস্তোঁরায় কোনো ওয়েটারের হাতে দেওয়া হয়, তখন তিনি এসব তথ্য নোট করতে পারেন এবং পরে একটি ব্যবহার করে ই-কমার্স সাইটে লেনদেন করতে পারেন।

কোনো ই-কমার্স সাইটে কার্ডের তথ্যের এ জাতীয় অননুমোদিত ব্যবহার রোধ করতে, কার্ড ইস্যুকারী ব্যাংক কার্ডধারীর কাছে একটি 2FA (দ্বি-ফ্যাক্টর অথেনটিকেশন) টোকেন সরবরাহ করতে পারে এবং ই-কমার্স অ্যাকুয়ারিং ব্যাংক অবশ্যই কার্ডের ঐ তিনটি তথ্যের সঙ্গে গ্রাহকের কাছে 2FA টোকেন নম্বর চাইবে। 2FA টোকেন নম্বরটি এককালীন নম্বর এবং এটি একটি পেন-ড্রাইভের মতো ডিভাইসে বা গ্রাহকের স্মার্টফোন/ল্যাপটপে ইনস্টল করা কোনো অ্যাপ্লিকেশন দ্বারা তৈরি হতে পারে। এটি ইস্যুকারী ব্যাংক থেকে কার্ডধারীর মোবাইলে প্রেরিত একটি ওটিপিও (এককালীন পাসওয়ার্ড) হতে পারে।

## ১.৫. বাহ্যিক ঝুঁকি / সাইবার হুমকি (External Risks/Cyber Threats)

### ১.৫.১. ডিস্ট্রিবিউটেড ডিনায়েল অব সার্ভিসেস (DDoS)

অজানা আক্রমণকারী দ্বারা একটি প্রতিষ্ঠানের ওয়েবসাইট, মেশিন বা কোনো ব্যাংকের নেটওয়ার্ক বন্ধ করে দেওয়াকে ডিডস্ আক্রমণ বলা হয়। এতে এগুলো গ্রাহকদের কাছে অপ্রাপ্য হয়ে পরে। উপযুক্ত নেটওয়ার্ক সুরক্ষা সিস্টেম স্থাপন করে কোনও ব্যাংকে ডিডিওএস আক্রমণ প্রতিরোধ করা যেতে পারে।

### ১.৫.১. র‍্যানসমওয়্যার (Ransomware)

র‍্যানসমওয়্যার হলো এক ধরনের দূষিত সফ্টওয়্যার, যা একটি মুক্তিপণ প্রদান না করা হলে তাদের সিস্টেম বা কম্পিউটারে ব্যবহারকারীদের অনুপ্রবেশকে বাধা

দেয়। দূষিত সফ্টওয়্যারটি প্রথমে কোনো ব্যাংকের কর্মচারীদের কাছে একটি আকর্ষণীয় অফারের বর্ণনা করে একটি ইমেলের সংযুক্তি হিসাবে প্রেরণ করা হয়। যদি কোনো অসচেতন ব্যবহারকারী ইমেল সংযুক্তিতে ক্লিক করেন তবে দূষিত সফ্টওয়্যারটি স্বয়ংক্রিয়ভাবে কম্পিউটারে ইনস্টল হয়ে যায়। সফ্টওয়্যারটি তখন WAN-এর মাধ্যমে সমস্ত কম্পিউটারে ছড়িয়ে পড়ে। তখন র‍্যানসমওয়্যারটি কম্পিউটারে সমস্ত বা নির্বাচিত ফাইলগুলো এনক্রিপ্ট করে ফেলে। ফাইলগুলো আনলক করার জন্য কম্পিউটারের মালিকের কাছে র‍্যানসম বা চাঁদা চাওয়া হয়। চাঁদা দিলে তারা কম্পিউটারটি আন-লক করে দেয়। সাধারণত বিটকয়েনের মতো ক্রিপ্টো-মুদ্রায় চাঁদা দেওয়া হয়।

ব্যাংকের কর্মীদের সচেতন করার লক্ষ্যে সচেতনতামূলক প্রোগ্রাম পরিচালনা করা যায়। ফলে তারা ইমেইলের সঙ্গে আগত অজানা সংযুক্তিতে ক্লিক করবেন না।

### ১.৫.৩. ম্যালওয়্যার (Malware)

ম্যালওয়্যার এমন একটি প্রোগ্রাম, যা ব্যবহারকারীর সম্মতি ছাড়াই অন্যান্য এক্সিকিউটেবল সফ্টওয়্যার (অপারেটিং সিস্টেমসহ)-এ সংযুক্ত হয়ে যায় এবং যখন ঐ সফ্টওয়্যারটি চালিত হয়, তখন ম্যালওয়্যারটি অন্যান্য এক্সিকিউটেবল সফ্টওয়্যারে ছড়িয়ে পড়ে।

ম্যালওয়্যারটি প্রথমে একটি ব্যাংকের কর্মকর্তাদের কাছে আকর্ষণীয় অফার বর্ণনা করে একটি ইমেলের সংযুক্তি হিসাবে প্রেরণ করা হয়। যদি কোনো অসচেতন ব্যবহারকারী ইমেইল সংযুক্তিতে ক্লিক করেন তবে ম্যালওয়্যারটি স্বয়ংক্রিয়ভাবে কম্পিউটারে ইনস্টল হয়ে যায়। ম্যালওয়্যার তারপরে হ্যাকারকে ব্যবহারকারী আইডি এবং পাসওয়ার্ডসহ সব সংবেদনশীল তথ্য প্রেরণ শুরু করে।

কম্পিউটারকে সংক্রামিত করার অন্য উপায়টিকে ফিশিং বলা হয়। ফিশিং একটি জাল ওয়েবসাইট যার চেহারা এবং যা দেখতে হুবহু সত্যিকারের ওয়েবসাইটের মতো এবং ব্যবহারকারী তা সত্যিকারের ওয়েবসাইট মনে করে তথায় তার ব্যক্তিগত তথ্য যেমন আইডি ও পাসওয়ার্ড প্রবেশ করান।

ওপরে উল্লিখিত উপায়গুলো মাধ্যমে প্রাপ্ত তথ্যের ব্যবহার করে, হ্যাকার ব্যবহারকারীর সংবেদনশীল সিস্টেমে অ্যাক্সেস করে এবং গ্রাহকের অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে টাকা স্থানান্তর করে অথবা হ্যাকড অ্যাকাউন্ট থেকে সরাসরি অর্থ তোলে নেয়।

ব্যাংকের কর্মচারীদের শিক্ষিত করার জন্য তাদের মধ্যে একটি সচেতনতা প্রোগ্রাম চালানো যেতে পারে—যাতে তারা ইমেইলগুলোর সঙ্গে অজানা সংযুক্তিতে ক্লিক না করে এবং তারা যথাযথ যাচাইকরণ ছাড়াই কোনো ওয়েবসাইটে তাদের ব্যবহারকারী আইডি ও পাসওয়ার্ড ইনপুট না করে।

### ১.৬. হ্যাকিং এবং অননুমোদিত অর্থ স্থানান্তর (Hacking and Unauthorized Transfer of money)

হ্যাকাররা ক্রমাগত বছরের পর বছর ধরে ব্যাংকিং সিস্টেমে অ্যাক্সেস পাওয়ার চেষ্টা করে। যদি তিনি সুরক্ষা ব্যবস্থায় কোনো ত্রুটি খুঁজে পেতে পারেন, তবে সেই লুফোলটি ব্যবহার করে হ্যাকার ব্যাংকিং নেটওয়ার্কে অ্যাক্সেস করেন। তারপরে তিনি কোনো গ্রাহকের অ্যাকাউন্ট থেকে অন্য ব্যাংক অ্যাকাউন্টে তহবিল স্থানান্তর করেন বা হ্যাকড অ্যাকাউন্ট থেকে সরাসরি অর্থ উত্তোলন করেন।

বাংলাদেশি টাকা অ-রূপান্তরযোগ্য (non-convertable)। সুতরাং সিবিএস (কোর ব্যাংকিং সিস্টেম) থেকে তহবিল স্থানান্তর আক্রমণকারী/হ্যাকারদের কাছে আকর্ষণীয় নয়। কোনো ক্লায়েন্টের অ্যাকাউন্ট থেকে হ্যাকারের অ্যাকাউন্টে তহবিল স্থানান্তর করার পরে, হ্যাকারদের বাংলাদেশের মধ্যে কোনো একটি ব্যাংকের শাখা বা এটিএম থেকে টাকা উত্তোলন করতে হবে এবং তারপরে টাকাকে একটি এক্সচেঞ্জ হাউস থেকে মার্কিন ডলারে রূপান্তর করতে হবে এবং অবশেষে, ব্যাগে করে সেই ডলার দেশের বাইরে নিতে হবে। প্রক্রিয়াটি জটিল এবং ঝুঁকিপূর্ণ। ফলে হ্যাকাররা বাংলাদেশি ব্যাংকের কোনো সিবিএস অ্যাকাউন্ট হ্যাক করতে কম আগ্রহী।

তবে, সুইফট সিস্টেম এবং ক্রেডিট কার্ড সিস্টেম গ্রাহকের ব্যালেন্সগুলো মার্কিন ডলারে বজায় থাকে। যদি হ্যাকাররা সুইফট বা ক্রেডিট কার্ড সিস্টেমে অ্যাক্সেস অর্জন করতে পারে তবে তারা বিশ্বের যে কোনও জায়গায় সরাসরি মার্কিন ডলার স্থানান্তর করতে পারে এবং সেই নির্দিষ্ট দেশ থেকে অর্থ উত্তোলন করতে পারে। তারা মার্কিন যুক্তরাষ্ট্রে অবস্থিত এটিএম থেকে ইউএসডলারও তোলতে পারে।

একটি ব্যাংকের আইটি সিকিউরিটি বিভাগকে ক্রমাগত বিভিন্ন ব্যর্থ হামলার ধরণ বিশ্লেষণ করা এবং ব্যাংকিং নেটওয়ার্ককে বিভিন্ন স্ট্রাটেজি প্রয়োগ করে শক্তিশালী এবং সুরক্ষিত করা প্রয়োজন।

### ১.৭. ক্রেডিট কার্ডের ডেটা চুরি (Stealing Credit Card Data)

হ্যাকাররা ডাটাবেস থেকে ক্রেডিট কার্ডের ডেটা চুরি করে। চুরি হওয়া ক্রেডিট কার্ডের ডেটা ব্যবহার করে, হ্যাকাররা জাল ক্রেডিট কার্ড তৈরি করে এবং পরে তারা সেটি পসে বিল প্রদানের জন্য বা এটিএম-এ টাকা তোলার জন্য ব্যবহার করে (বাংলাদেশে টাকা বা অন্যান্য দেশে অন্যান্য মুদ্রা পান)।

ব্যাংকের আইটি সিকিউরিটি বিভাগ দ্বারা উপযুক্ত নেটওয়ার্ক সিকিউরিটি সিস্টেম ইনস্টল করে হ্যাকারদের ক্রেডিট কার্ডের ডেটা চুরি করা থেকে বিরত রাখতে পারে।

### ১.৮. ক্রিপ্টো-কারেন্সি হুমকি (Crypto-currency Threats)

ক্রিপ্টোকারেন্সি হলো নগদ অর্থের একটি ইলেকট্রনিক সংস্করণ। কিছু ক্রিপ্টো-কারেন্সির উদাহরণ হলো বিটকয়েন, ইথার, লাইটকয়েন, মনেরো, ড্যাশ, পঞ্জিকয়েন, জেডক্যাশ, কার্বন, টিথার ও পেট্রো। একটি ক্রিপ্টো-মুদ্রার মালিক সিস্টেমে বেনামী থাকে (যেহেতু অনবোর্ডিংয়ের সময় ব্যবহারকারীর জন্য কোনো KYC করা হয় না) এবং এটি বিভিন্ন অবৈধ কার্যকলাপ যেমন ড্রাগ এবং অন্যান্য অবৈধ পণ্য কেনা, মুক্তিপণ প্রদান, মানব পাচারের অর্থ স্থানান্তর এবং সংগঠিত সন্ত্রাসী গোষ্ঠীকে অর্থ প্রদান করার জন্য ব্যবহৃত হয়। ক্রিপ্টো-কারেন্সির কিছু পটভূমি হলো—

- এটি কোনো কেন্দ্রীয় ব্যাংক দ্বারা নিয়ন্ত্রিত হয় না।
- এর কোনো ভৌগোলিক সীমানা নেই।
- ব্যবহারকারীদের কোনো KYC-এর প্রয়োজন হয় না।
- এর কোনো নির্দিষ্ট কর্তৃপক্ষ নেই, ফলে কোনো ভোক্তা সুরক্ষার ব্যবস্থা নেই এবং কোন AMT/CFT প্রতিবেদন প্রদান করতে হয় না।
- প্রকৃত অর্থের মতো, একটি ক্রিপ্টোকারেন্সির মূল্য কোনো সম্পদ (asset) দ্বারা সমর্থিত নয়।

ফলে ক্রিপ্টো-কারেন্সি একটি মুদ্রা হতে ব্যর্থ হয়েছে।

ক্রিপ্টো-কারেন্সির প্রধান হুমকি হলো মানি লন্ডারিং ও সন্ত্রাসী অর্থায়ন (এমএলটিএফ) সংক্রান্ত ঝুঁকি।

### ১.৯. আইটি ঝুঁকি কমাতে কী করতে হবে?

ব্যাংকিং অটোমেশন থেকে উদ্ভূত হুমকিগুলো কমাতে, ব্যাংকগুলোকে একটি স্বাধীন আইটি সিকিউরিটি বিভাগ (এমডি এবং সিইওর অধীনে) স্থাপন করতে হবে। এছাড়াও ব্যাংকগুলোকে নিম্নলিখিতগুলো নিশ্চিত করতে হবে—

- পূর্ণসংখ্যক সার্ভার, সরঞ্জাম এবং নেটওয়ার্কিংয়ের সুবিধাসহ উপযুক্ত স্থানে ডেটা সেন্টার, ডিআরএস এবং নিয়ার ডেটা সেন্টার সেট আপ করা।
- কর্মচারী সচেতনতা কার্যক্রম পরিচালনা করা।
- সুগঠিত আইটি অবকাঠামো স্থাপন করা।
- পিসিআই-ডিএসএস এবং আইএসও২৭কে সার্টিফিকেশনপ্রাপ্তি।
- নিম্নলিখিত নেটওয়ার্ক সরঞ্জামগুলো সঠিকভাবে স্থাপন এবং কনফিগার করা।
  - ফায়ারওয়াল।
  - আইপিএস।
  - WAF (ওয়েব অ্যাপ্লিকেশন ফায়ারওয়াল)।
  - ইমেল সিকিউরিটি গেটওয়ে।
  - ওয়েব সিকিউরিটি গেটওয়ে।
- পাইরেটেড সফটওয়্যার ব্যবহার না করা।
- নিয়মিত ড্রাইভার হালনাগাদ করা।
- নিয়মিত প্যাচ পর্যালোচনা করা।
- জিরো-ডে অ্যাটাক্ট (স্যান্ডবক্সিং) বন্ধ করার ব্যবস্থা গ্রহণ করা এবং
- নিয়মিত সাইবার নিরাপত্তা বিশেষজ্ঞদের মাধ্যমে তদন্ত করা।

### ২. সাইবার নিরাপত্তা (Cyber Security)

সাইবার নিরাপত্তা হলো একটি নিরাপত্তা ব্যবস্থা, যা সাধারণত ইন্টারনেট ব্যবহার করে অননুমোদিত বহিরাগত ইলেকট্রনিক অ্যাক্সেস থেকে একটি সংস্থার ডেটা এবং তথ্য রক্ষা করতে ব্যবহৃত হয়। সাইবার নিরাপত্তা হলো আইসিটি নিরাপত্তার একটি উপসেট। ছোট ব্যবসাগুলো সাইবার হুমকির জন্য বেশি ঝুঁকিপূর্ণ। কারণ সম্ভাব্য হ্যাকাররা জানে যে ছোট ব্যবসাগুলোর যথেষ্ট পরিমাণে সম্পদের অভাব রয়েছে। বড় কর্পোরেশনগুলো যেমন নিরাপত্তা প্রযুক্তি এবং কৌশলগুলোতে বিনিয়োগ করতে পারে, ছোট ব্যবসাগুলো তা পারে না। ডিজিটাল নেটওয়ার্ক রক্ষাকারীর নিরাপত্তা পদ্ধতি এবং নীতিগুলো দ্রুত পরিবর্তিত হয়, তাই সাইবার হুমকির বিরুদ্ধে তাদের সাইবারস্পেসকে আরও ভালোভাবে রক্ষা করার জন্য ব্যবসা প্রতিষ্ঠানগুলোকে সাম্প্রতিক সাইবার নিরাপত্তা ব্যবস্থাগুলোর সঙ্গে হালনাগাদ থাকতে হবে। কিছু সাধারণ সাইবার আক্রমণের মধ্যে রয়েছে ফিশিং, ডেটা ব্রিচিং, প্রলোভন ইত্যাদি। এগুলো পূর্ববর্তী অধ্যায়ে আলোচনা করা হয়েছে।

### ৩. আইসিটি ঝুঁকি ব্যবস্থাপনা (ICT Risk Management)

আইসিটি ঝুঁকি ব্যবস্থাপনা হলো, একটি সংস্থার আইসিটি সিস্টেমগুলোকে রক্ষা করার জন্য তৈরি করা অপরিহার্য প্রক্রিয়া। বাংলাদেশের কেন্দ্রীয় ব্যাংকের প্রয়োজনীয়তা অনুযায়ী, আইসিটি ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার অংশ হিসাবে, বাংলাদেশের প্রতিটি ব্যাংক এবং এনবিএফআইকে তাদের নিজ নিজ আইসিটি নীতিমালা তৈরি করতে হবে, তাদের নিজ নিজ পরিচালনা পর্ষদের অনুমোদন নিতে হবে এবং তা বাস্তবায়ন করতে হবে।

## ৪. নিরাপত্তার স্ট্যান্ডার্ড ও প্রবিধান (Security Standards and Regulations)

বিশ্বজুড়ে অনেক সরকার স্ট্যান্ডার্ড (যা এন্টারপ্রাইজগুলো তাদের আইটি নিরাপত্তা উন্নত করতে অনুসরণ করতে পারে) / প্রবিধান (যা জরিমানা এড়াতে এন্টারপ্রাইজগুলো অবশ্যই অনুসরণ করবে) প্রস্তুত করছে যাতে রয়েছে কোম্পানিগুলো কীভাবে তথ্য সুরক্ষা পরিচালনা এবং নিয়ন্ত্রণ করবে। লক্ষ্যটি সহজ : ব্যবস্থাপনা ও পরিচালনা পর্ষদকে তথ্য সুরক্ষার জন্য দায়ী হতে বাধ্য করা এবং তাদের সম্পদ রক্ষার জন্য তারা যে ডিউ ডেলিজেন্স প্রদর্শন করে তা যেন আইটি সম্পদ রক্ষায় প্রয়োগ করে।

এই ধরনের প্রবিধানগুলোর মধ্যে রয়েছে ২০০২ সালের Sarbanes-oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA) এবং স্বাস্থ্য ইন্সুরেন্স পোর্টেবিলিটি অ্যান্ড অ্যাকাউন্টেবিলিটি অ্যাক্ট অব ১৯৯৬ (HIPAA), ইউএসএ পেট্রিওট অ্যাক্ট, কানাডা PIPEDA এবং স্ট্যান্ডার্ডগুলোর মধ্যে রয়েছে BS7799, বাংলাদেশ ব্যাংক (বাংলাদেশের কেন্দ্রীয় ব্যাংক) দ্বারা প্রণীত 'তফশিলি ব্যাংক এবং আর্থিক প্রতিষ্ঠানের জন্য আইসিটি নিরাপত্তা সংক্রান্ত নির্দেশিকা' এবং অনেক জাতীয় স্ট্যান্ডার্ড।

কিছু নিরাপত্তা স্ট্যান্ডার্ড/প্রবিধানের সংক্ষিপ্ত তুলনা নিচে দেওয়া হল—

| নিরাপত্তা স্ট্যান্ডার্ড/প্রবিধান | কে মেনে চলবে? | নিরাপত্তা বিধান কী কী অন্তর্ভুক্ত করে? | জরিমানা কী? | কখন থেকে তা প্রযোজ্য? |
|---|---|---|---|---|
| Sarbanes-Oxley Act, 2002 | সমস্ত পাবলিক কোম্পানি (মার্কিন নিরাপত্তা আইন সাপেক্ষে) | অভ্যন্তরীণ নিয়ন্ত্রণ এবং আর্থিক ডিসক্লোজার | ক্রিমিনাল ও সিভিল পেনাল্টি | বর্তমান আইন |
| Gramm-Leach-Bliley Act, 1999 | আর্থিক প্রতিষ্ঠান | গ্রাহক রেকর্ডের নিরাপত্তা | ক্রিমিনাল ও সিভিল পেনাল্টি | বর্তমান আইন |
| Health Insurance Portability & Accountability Act (HIPAA) | স্বাস্থ্য পরিকল্পনা, স্বাস্থ্যসেবা ক্লিয়ারিং হাউস এবং স্বাস্থ্যসেবা প্রদানকারী প্রতিষ্ঠান | ইলেকট্রনিক আকারে ব্যক্তিগত স্বাস্থ্য তথ্য | সিভিল ফাইল ও ক্রিমিনাল পেনাল্টি | বর্তমান আইন |
| বিএস৭৭৯৯/ আইএসও ১৭৭৯৯ | আইটি নিরাপত্তা উন্নত করতে আগ্রহী যেকোনো প্রতিষ্ঠান | যেকোন এন্টারপ্রাইজের ইনফরমেশন সিকিউরিটি ম্যানেজমেন্ট সিস্টেম (ISMS) | কোনো আইন নয়, তাই কোনো জরিমানা নেই | বর্তমান সিকিউরিটি স্ট্যান্ডার্ড |
| তফসিলি ব্যাংক এবং আর্থিক প্রতিষ্ঠানের জন্য আইসিটি নিরাপত্তা সংক্রান্ত নির্দেশিকা | বাংলাদেশে ব্যাংক ও আর্থিক প্রতিষ্ঠান | আইটি সম্পদ এবং গ্রাহক তথ্যের নিরাপত্তা | আইন নয়, তাই শাস্তির বিধান নেই | বর্তমান সিকিউরিটি স্ট্যান্ডার্ড |
| পিসিআই-ডিএসএস | ডেবিট এবং ক্রেডিট কার্ড নিয়ে কাজ করে এমন কোনো প্রতিষ্ঠান। | কার্ড সম্পর্কিত তথ্য এবং তথ্যের প্রবাহ এবং স্টোরেজ সুরক্ষিত করা | আইন নয়, তাই শাস্তির বিধান নেই | বর্তমান সিকিউরিটি স্ট্যান্ডার্ড |
| আইএসও ২৭০০০ | আইটি সিস্টেম এবং নিরাপত্তা উন্নত করতে আগ্রহী যে কোন প্রতিষ্ঠান | যেকোনো এন্টারপ্রাইজের আইসিটি সিস্টেম | আইন নয়, তাই শাস্তির বিধান নেই | বর্তমান সিকিউরিটি স্ট্যান্ডার্ড |

যেসব প্রতিষ্ঠান এসব স্ট্যান্ডার্ড ও প্রবিধান মেনে চলে, তারা ইতোমধ্যেই একটি শক্ত ও বাস্তব ইনফরমেশন সিকিউরিটি সিস্টেম বাস্তবায়ন করে ফেলেছে।

উদাহরণস্বরূপ, HIPAA ব্যক্তিগত তথ্য সুরক্ষার ওপর জোর দেওয়ার সময় আইএসও১৭৭৯৯ স্ট্যান্ডার্ডের মতো একই বিষয়গুলোকে মেনে চলে। আইএসও ১৭৭৯৯ এবং বিএস ৭৭৯৯-২-এর কমপ্লায়েন্স মানে কোম্পানি সংবেদনশীল তথ্যের নিরাপত্তার জন্য নীতি এবং পদ্ধতির সংজ্ঞা নির্ধারণ করেছে, যা SOX-এ বর্ণিত আছে।

এই অধ্যায়ে আমরা নিরাপত্তার স্ট্যান্ডার্ড নিয়ে আলোচনা করব, বিশেষ করে বাংলাদেশ ব্যাংক দ্বারা প্রকাশিত 'তফসিল ব্যাংক এবং আর্থিক প্রতিষ্ঠানের জন্য

আইসিটি নিরাপত্তা সংক্রান্ত নির্দেশিকা' এবং বিএস৭৭৯৯ ও আইএসও ২৭০০০ সম্পর্কে।

**একটি নিরাপত্তার স্ট্যান্ডার্ড মেনে চলার সুবিধাগুলো হলো**

স্পষ্টতই, একটি সিকিউরিটি স্ট্যান্ডার্ড মেনে চলা এবং একটি নির্দিষ্ট স্ট্যান্ডার্ডের সার্টিফিকেট অর্জন করা প্রমাণ করে না যে প্রতিষ্ঠানটি ১০০% নিরাপদ। সত্য হলো, সমস্ত কার্যকলাপ বন্ধ করা ছাড়া, সম্পূর্ণ নিরাপত্তা বলে কিছু নেই। তবুও একটি স্ট্যান্ডার্ড গ্রহণ করলে কিছু সুবিধা পাওয়া যায়, যার মধ্যে রয়েছে—

**ক) সাংগঠনিক পর্যায়ে (At the Organizational Level)**

প্রতিশ্রুতি : সার্টিফিকেশন সংস্থাটিকে সমস্ত স্তরে সুরক্ষিত করার জন্য যথেষ্ট চেষ্টা করা হয়েছে এবং প্রশাসকদের দ্বারা 'ডিউ ডেলিজেন্স' করা হয়েছে, তা বোঝায়।

**খ) আইনি স্তরে (At the Legal Level)**

কমপ্লায়েন্স : সার্টিফিকেশন উপযুক্ত কর্তৃপক্ষের কাছে সংস্থা কর্তৃক প্রযোজ্য আইন ও প্রবিধান প্রতিপালন করছে, তা বোঝায়।

**গ) অপারেটিং স্তরে (At the Operating Level)**

ঝুঁকি ব্যবস্থাপনা : ইনফরমেশন সিস্টেম, তাদের দুর্বলতা এবং কীভাবে তাদের রক্ষা করা যায় এটি সে সম্পর্কে আরও ভালো জ্ঞান প্রদান করে। একইভাবে এটি হার্ডওয়্যার এবং ডেটা উভয়েরই আরও নির্ভরযোগ্য প্রাপ্যতা নিশ্চিত করে।

**ঘ) বাণিজ্যিক পর্যায়ে (At the Commercial Level)**

বিশ্বাসযোগ্যতা এবং আত্মবিশ্বাস : অংশীদার, শেয়ারহোল্ডার এবং গ্রাহকরা আশ্বস্ত হন যখন তারা তথ্য সুরক্ষার জন্য সংস্থার প্রদত্ত 'গুরুত্ব' দেখেন। সার্টিফিকেশন একটি কোম্পানিকে তার প্রতিযোগীদের থেকে এবং বাজারে আলাদা করতে সাহায্য করতে পারে।

**ঙ) আর্থিক স্তরে (At the Financial Level)**

নিরাপত্তা লঙ্ঘন সম্পর্কিত খরচ হ্রাস, এবং বীমা প্রিমিয়ামের সম্ভাব্য হ্রাস করে

চ) মানব পর্যায়ে (At the Human Level)

সংস্থার ভেতরে নিরাপত্তা সমস্যা এবং কর্মকর্তাদের দায়িত্ব সম্পর্কে সচেতনতা বৃদ্ধি করে।

## ৫. বাংলাদেশ কেন্দ্রীয় ব্যাংক (২০১৫) দ্বারা প্রকাশিত তফসিলি ব্যাংক এবং আর্থিক প্রতিষ্ঠানের জন্য আইসিটি নিরাপত্তা সংক্রান্ত নির্দেশিকা

সাম্প্রতিক বছরগুলোতে ব্যাংকসমূহ গ্রাহকদের পরিষেবা প্রদান এবং তথ্য প্রক্রিয়াকরণের উপায়ে যথেষ্ট পরিবর্তন করেছে। তথ্য ও যোগাযোগ প্রযুক্তি (আইসিটি) এই গুরুত্বপূর্ণ পরিবর্তনটি এনেছে। ইলেকট্রনিক ব্যাংকিং আরও জনপ্রিয় হয়ে উঠছে এবং আর্থিক অন্তর্ভুক্তিতে ব্যাংকগুলো আরও বেশি মনোযোগী হয়েছে। তাই আর্থিক প্রতিষ্ঠানগুলোর জন্য তথ্যের নিরাপত্তা অনেক বেশি গুরুত্ব পেয়েছে এবং ঝুঁকিগুলো সঠিকভাবে চিহ্নিত ও পরিচালনা করা আমাদের জন্য অত্যাবশ্যক।

অধিকন্তু, তথ্য ও তথ্য প্রযুক্তি সিস্টেমগুলো ব্যাংক এবং নন-ব্যাংক আর্থিক প্রতিষ্ঠানের (NBFI) পাশাপাশি তাদের গ্রাহক এবং স্টেকহোল্ডারদের জন্য অপরিহার্য সম্পদ। তথ্য সম্পদগুলো ব্যাংক ও এনবিএফআই দ্বারা তাদের গ্রাহকদের দেওয়া পরিষেবাগুলোর জন্য গুরুত্বপূর্ণ। এই সম্পদগুলোর সুরক্ষা এবং রক্ষণাবেক্ষণ সংস্থার স্থায়িত্বের জন্য গুরুত্বপূর্ণ। ব্যাংক এবং এনবিএফআইগুলোকে অবশ্যই অননুমোদিত অ্যাক্সেস, পরিবর্তন, প্রকাশ এবং ধ্বংস থেকে তথ্য রক্ষা করার দায়িত্ব নিতে হবে। পরিষেবার দিকে পরিচালিত ব্যবসার জন্য ব্যাংক এবং এনবিএফআই-এর পদ্ধতিগুলো ঝুঁকিভিত্তিক, যার মানে আইসিটি ঝুঁকিও ব্যাংকিং ব্যবস্থার সঙ্গে যুক্ত এবং চিন্তাভাবনা ও প্রচেষ্টার সঙ্গে পরিচালনা করা প্রয়োজন। এর পরিপ্রেক্ষিতে, ব্যাংক এবং এনবিএফআই দ্বারা অনুসরণ করার জন্য বাংলাদেশ ব্যাংক ২০১৫ সালে আইসিটি নিরাপত্তা সংক্রান্ত একটি নির্দেশিকা তৈরি করেছিল। নির্দেশিকাটির বিশেষ বিশেষ বৈশিষ্ট্যগুলো এই অধ্যায়ে আলোচনা করা হলো।

### ৫.১. ব্যাংক এবং এনবিএফআইগুলোর শ্রেণিকরণ (Categoization of Banks and NBFIs)

কোর ব্যাংকিং অ্যাপ্লিকেশন সফটওয়্যারের স্থাপত্যে, আইসিটি অবকাঠামো, কর্মক্ষম পরিবেশ এবং পদ্ধতির ওপর নির্ভর করে, একটি ব্যাংক বা এসবিএফআই কে নিম্নরূপে শ্রেণিবদ্ধ করা যেতে পারে—

ক্যাটাগরি-১ : যে ব্যাংকের একটি ডেটা সেন্টার রয়েছে এবং গুরুত্বপূর্ণ সেবাসমূহ অব্যাহত রাখার উদ্দেশ্যে বেকআপ সিস্টেমসহ একটি ডিআরএসও রয়েছে এবং এর মাধ্যমে কোর ব্যাংকিং সিস্টেম পরিচালনা করার জন্য একটি সেন্ট্রালাইজড আইসিটি অপারেশন রয়েছে। এই সিস্টেমে ব্যাংকের সমস্ত অফিস, শাখা ও বুথ WAN-এর মাধ্যমে ২৪x৭ ঘণ্টা সংযুক্ত থাকে।

ক্যাটাগরি-২ : যে ব্যাংক ডি-সেন্ট্রালাইজ অপারেশন পরিচালনা করে থাকে। এক্ষেত্রে ডিস্ট্রিবিউটেড অ্যাপ্লিকেশনসমূহ ডেটা সেন্টারে বা অপারেশনাল অফিসে

ব্যাকআপ সুবিধাসহ ইন্‌স্টল করা হয়। ব্যাংকের অফিস, শাখা বা বুথ WAN-এর মাধ্যমে সংযুক্ত থাকতে পারে বা স্ব স্ব অফিসে স্ট্যান্ড অ্যালোন আকারে থাকতে পারে।

### ৫.২. আইসিটি নিরাপত্তা ব্যবস্থাপনা (ICT Security Management)

আইসিটি সিকিউরিটি ম্যানেজমেন্টকে অবশ্যই নিশ্চিত করতে হবে যে আইসিটি ফাংশন ও অপারেশনগুলো দক্ষতার সঙ্গে এবং কার্যকরভাবে পরিচালিত হয়। ব্যাংক এবং এনবিএফআই আইসিটি এর ক্ষমতা সম্পর্কে সচেতন হবে এবং সম্ভাব্য অপব্যবহারের সুযোগ এবং ঝুঁকিগুলো উপলব্ধি করতে এবং স্বীকৃতি দিতে সক্ষম হবে। তাদের যথাযথ সিস্টেম ডকুমেন্টেশনের রক্ষণাবেক্ষণ নিশ্চিত করতে হবে, বিশেষ করে সিস্টেমের জন্য, যা আর্থিক লেনদেন এবং রিপোর্টিং সমর্থন করে। তাদের আইসিটি নিরাপত্তা পরিকল্পনায় অবদান রাখতে হবে—যাতে ব্যবসায়িক উদ্দেশ্যের সঙ্গে ধারাবাহিকভাবে সম্পদ বরাদ্দ করা হয় এবং পর্যাপ্ত এবং যোগ্য কারিগরি কর্মীদের নিযুক্ত করা হয়। এটি নিশ্চিত করবে যে আইসিটি অপারেশনের ধারাবাহিকতা ঝুঁকির মধ্যে থাকবে না। আইসিটি নিরাপত্তা ব্যবস্থাপনার প্রধান দায় এবং দায়িত্ব হলো, আইসিটি নিরাপত্তা নীতি, ডকুমেন্টেশন, অভ্যন্তরীণ এবং বাহ্যিক সিস্টেম অডিট, প্রশিক্ষণ এবং সচেতনতা, বীমা বা ঝুঁকি কভারেজ তহবিল নিয়ে কাজ করা।

### ৫.২.১. দায় ও দায়িত্ব (Roles and Responsibilities)

আইসিটি গভর্নেন্স বাস্তবায়নের সময় বোর্ড এবং সিনিয়র ম্যানেজমেন্টের দায় এবং দায়িত্বগুলো সংজ্ঞায়িত করা গুরুত্বপূর্ণ, কিন্তু স্পষ্টভাবে সংজ্ঞায়িত দায় ও দায়িত্ব ভূমিকা কার্যকর প্রকল্প নিয়ন্ত্রণ এবং সংস্থাগুলোর প্রত্যাশা পূরণে সহায়ক ভূমিকা পালন করে। আইসিটি গভর্নেন্স স্টেকহোল্ডারদের মধ্যে রয়েছে পরিচালনা পর্ষদ, সিইও, আইসিটি স্টিয়ারিং কমিটি, আইসিটি নিরাপত্তা কমিটি, সিআইও, সিটিও, সিআইএসও, ঝুঁকি ব্যবস্থাপনা কমিটি, প্রধান ঝুঁকি কর্মকর্তা ও ব্যবসায়িক নির্বাহীরা।

#### i) পরিচালনা পর্ষদের দায় ও দায়িত্ব

ক) আইসিটি কৌশল ও নীতিমালা অনুমোদন করা।
খ) ব্যবস্থাপনা উপযুক্ত কার্যকর পরিকল্পনা প্রক্রিয়া স্থাপন করেছে, তা নিশ্চিত করা।
গ) নিশ্চিত করা যে, আইসিটি কৌশলটি প্রকৃতপক্ষে ব্যবসায়িক কৌশলের সঙ্গে সামঞ্জস্যপূর্ণ।
ঘ) নিশ্চিত করা যে, আইসিটি সাংগঠনিক কাঠামো ব্যবসায়িক মডেল এবং এর দিকনির্দেশের পরিপূরক।
ঙ) আইসিটি বিনিয়োগ এমনভাবে করা, যাতে ঝুঁকি এবং সুবিধার ভারসাম্য ও গ্রহণযোগ্য বাজেটের প্রতিনিধিত্ব করে।
চ) আইসিটি নিরাপত্তা নীতির কমপ্লায়েন্স নিশ্চিত করা।

#### ii) আইসিটি স্টিয়ারিং কমিটির দায় ও দায়িত্ব

আইসিটি, রিস্ক, এইচআর, আইসিসি/অডিট, আইন এবং অন্যান্য সংশ্লিষ্ট ব্যবসায়িক ইউনিটের প্রতিনিধিদের নিয়ে আইসিটি স্টিয়ারিং কমিটি গঠন করা প্রয়োজন। এটির কাজ হলো—

ক) কৌশলগত লক্ষ্য নির্ধারণ এবং অর্জনের জন্য ব্যবস্থাপনা পদ্ধতি পর্যবেক্ষণ করুন।
খ) আইসিটি ঝুঁকি এবং নিয়ন্ত্রণের প্রতি এক্সপোজার সম্পর্কে সচেতন হওয়া।
গ) ঝুঁকি, তহবিল বা সোর্সিং সম্পর্কিত নির্দেশিকা প্রদান করা।
ঘ) প্রকল্পের অগ্রাধিকার এবং আইসিটি প্রস্তাবের সম্ভাব্যতা মূল্যায়ন নিশ্চিত করা।
ঙ) নিশ্চিত করা যে, সমস্ত ক্রিটিক্যাল প্রকল্পে 'প্রকল্প ঝুঁকি ব্যবস্থাপনা' এর জন্য একটি অংশ রয়েছে।
চ) মানদণ্ডের মধ্যে প্রযুক্তি নির্বাচনের বিষয়ে পরামর্শ প্রদান।
ছ) নিশ্চিত করা যে, নতুন প্রযুক্তির দুর্বলতা মূল্যায়ন করা হয়েছে।
জ) নিয়ন্ত্রক ও সংবিধিবদ্ধ প্রয়োজনীয়তাগুলোর কমপ্লায়েন্স নিশ্চিত করা।
ঝ) স্থাপত্য নকশার দিকনির্দেশ প্রদান করা এবং নিশ্চিত করা যে আইসিটির ডিজাইন আর্কিটেকচার আইনি এবং নিয়ন্ত্রকের কমপ্লায়েন্স পরিপালন করে।

#### iii) আইসিটি নিরাপত্তা কমিটির দায় ও দায়িত্ব

আইসিটি, আইসিটি সিকিউরিটি, রিস্ক, আইসিসি ও ব্যবসায়িক ইউনিটের প্রতিনিধিদের নিয়ে আইসিটি নিরাপত্তা কমিটি গঠন করতে হবে। এর কাজ হলো :

ক) আইসিটি নিরাপত্তার উদ্দেশ্য, আইসিটি নিরাপত্তা সংক্রান্ত নীতি ও পদ্ধতির উন্নয়ন ও বাস্তবায়ন নিশ্চিত করা।
খ) তথ্য সুরক্ষা প্রক্রিয়াগুলোতে চলমান ব্যবস্থাপনা সহায়তা প্রদান করা।
গ) আইসিটি নিরাপত্তা সম্পর্কিত ব্যবসায়িক উদ্দেশ্য, নিয়ন্ত্রক এবং আইনি প্রয়োজনীয়তাগুলোর সঙ্গে অব্যাহত কমপ্লায়েন্স নিশ্চিত করুন।

ঘ) আইসিটি ঝুঁকি ব্যবস্থাপনা কাঠামো/প্রক্রিয়া প্রণয়ন এবং গ্রহণযোগ্য আইসিটি ঝুঁকি থ্রেশহোল্ড/আইসিটি ঝুঁকি অ্যাপাটাইট এবং অ্যাশোরেন্স স্থাপনে সহায়তা করা।

ঙ) পর্যায়ক্রমিক পর্যালোচনা ও আইসিটি সুরক্ষা প্রক্রিয়াগুলোতে পরিবর্তনের জন্য অনুমোদন প্রদান।

### ৫.২.২ আইসিটি নীতি, স্ট্যান্ডার্ড এবং পদ্ধতি (ICT Policy, Standard and Procedure)

i) প্রতিটি ব্যাংক বা এনবিএফঅআই-এর অবশ্যই এই আইসিটি নিরাপত্তা নির্দেশিকার আলোকে একটি 'আইসিটি নিরাপত্তা নীতি' থাকতে হবে এবং বোর্ড দ্বারা তা অনুমোদিত হতে হবে।

ii) ব্যাংক বা এনবিএফআই এবং সামগ্রিক শিল্প উভয় ক্ষেত্রেই আইসিটি পরিবেশে ক্রমবর্ধমান পরিবর্তনগুলো মোকাবেলা করার জন্য নীতির নিয়মিত হালনাগাদ করতে হবে।

iii) ব্যাংক বা এনবিএফআই পৃথক আইসিটি নিরাপত্তা বিভাগ/ইউনিট/সেলে নিয়োজিত আইসিটি নিরাপত্তা পেশাদারদের নিরাপত্তা সংক্রান্ত ঘটনা, নীতিগত ডকুমেন্টেশন, অন্তর্নিহিত আইসিটি ঝুঁকি, ঝুঁকির ব্যবস্থাপনা এবং অন্যান্য প্রাসঙ্গিক কার্যক্রম দক্ষভাবে পরিচালনা/মোকাবিলা করার নিমিত্তে নিযুক্ত করতে হবে।

iv) নন-কমপ্লায়েন্স সমস্যাগুলোর ক্ষেত্রে দ্রুত কমপ্লায়েন্স প্লান তৈরি করে বাংলাদেশ ব্যাংকে জমা দিতে হবে। একটি নির্দিষ্ট সময়ের জন্য বাংলাদেশ ব্যাংক ডিস্পেনসেশন দিতে পারে।

### ৫.২.৩. ডকুমেন্টেশন (Documentation)

i) ব্যাংক বা এনবিএফআই তাদের আইসিটি বিভাগের জন্য অর্গানোগ্রাম হালনাগাদ করবে।

ii) ব্যাংক বা এনবিএফআই এর অর্গানোগ্রামে আইসিটি সহায়তা ইউনিট/বিভাগ থাকতে হবে।

iii) আইসিটি বিভাগ/ইউনিট/সেকশনের প্রত্যেক ব্যক্তির ফলব্যাক কাজের বিবরণ (জেডি) অনুমোদিত থাকবে। জব-ডেস্ক্রিপশনের সঙ্গে ফলব্যাক রিসোর্স পার্সনের নাম থাকতে হবে।

iv) ব্যাংক বা এনবিএফআই আইসিটি কাজের জন্য দায়িত্বের পৃথকীকরণ বজায় রাখবে।

v) ব্যাংক বা এনবিএফআই সমস্ত আইসিটি আদর্শ বা ক্রিটিকাল সিস্টেম/পরিষেবাগুলোর জন্য বিশদ নকশা বজায় রাখবে (যেমন ডেটা সেন্টার ডিজাইন, নেটওয়ার্ক ডিজাইন, ডেটা সেন্টারের জন্য পাওয়ার লেআউট, ইত্যাদি)।

vi) সংবেদনশীল আইসিটি কাজের জন্য ব্যাংক বা এনবিএফআই-এর পূর্বনির্ধারিত রোস্টার থাকতে হবে (যেমন, ইওডি অপারেশন, নেটওয়ার্ক মনিটরিং, সিকিউরিটি মনিটারিং, ডেটা সেন্টারের জন্য সিকিউরিটি গার্ড, এটিএম মনিটরিং ইত্যাদি)।

vii) ব্যাংক বা এনবিএফআই সকল আইসিটি কার্যক্রমের জন্য হালনাগাদ 'অপারেটিং পদ্ধতি' বজায় রাখবে (যেমন ব্যাকআপ ম্যানেজমেন্ট, ডাটাবেস ম্যানেজমেন্ট, নেটওয়ার্ক ম্যানেজমেন্ট, শিডিউলিং প্রসেস, সিস্টেম স্টার্ট-আপ, শাট-ডাউন, রিস্টার্ট ও রিকভারি)।

viii) বিভিন্ন আইসটি অনুরোধ/অপারেশন/পরিষেবার জন্য ব্যাংক বা এনবিএফআই-এর প্রাসঙ্গিক রিকুইজিশন/একনলেজম্যান্ট ফর্ম অনুমোদিত হতে হবে।

ix) ব্যাংক বা এনবিএফআই-এর কাছে অভ্যন্তরীণ/বাহ্যিক ব্যবহারকারীদের জন্য সমস্ত অ্যাপ্লিকেশনের ব্যবহারকারী ম্যানুয়াল থাকতে হবে।

### ৫.২.৪. অভ্যন্তরীণ ইনফরমেশন সিস্টেম নিরীক্ষা (Internal Information System Audit)

i) ইন্টারনাল ইনফরমেশন সিস্টেম (আইএস) অডিট, ব্যাংক বা NBFI-এর অভ্যন্তরীণ নিরীক্ষা বিভাগ দ্বারা পরিচালিত হবে।

ii) অভ্যন্তরীণ আইএস অডিট পর্যাপ্ত আইএস অডিট দক্ষতা সম্পন্ন কর্মীদের দ্বারা পরিচালিত হবে। প্রযুক্তির এক্ষেত্রে পর্যাপ্ত নিরীক্ষার অভিজ্ঞতা সম্পন্ন সার্টিফায়েড আইএস নিরীক্ষকের নিযুক্তি প্রশংসনীয় হতে পারে।

iii) ব্যাংক বা এনবিএফআই আইএস অডিট মূল্যায়ন, ডেটা নিষ্কাশন/বিশ্লেষণ, জালিয়াতি পর্যবেক্ষণ/অডিটিং, নিয়ন্ত্রণ পরিকল্পনা, শনাক্তকরণ/প্রতিরোধ ও ব্যবস্থাপনার জন্য কম্পিউটার-অ্যাসিস্টেড-অডিটিং টুলস (CAATs) ব্যবহার করতে পারে।

iv) একটি বার্ষিক সিস্টেম অডিট পরিকল্পনা তৈরি করা যেতে পারে, যার মধ্যে গুরুত্বপূর্ণ/প্রধান প্রযুক্তিভিত্তিক পরিষেবা/প্রক্রিয়া ও আইসিটি পরিকাঠামোসহ অপারেশনাল শাখাগুলো অন্তর্ভুক্ত থাকবে।

v) অভ্যন্তরীণ তথ্য সিস্টেম নিরীক্ষা বছরে অন্তত একবার পর্যায়ক্রমে করা হবে। প্রতিবেদনটি নিয়ন্ত্রকদের জন্য সংরক্ষণ করতে হবে এবং যখন প্রয়োজন তখন তাদেরকে দেখাতে হবে। এছাড়াও ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে অডিট সমস্যাগুলো সঠিকভাবে ট্র্যাক করা হয়েছে এবং বিশেষ করে, সম্পূর্ণভাবে রেকর্ড করা হয়েছে, পর্যাপ্তভাবে অনুসরণ করা হয়েছে এবং সন্তোষজনকভাবে সংশোধন করা হয়েছে।

vi) ব্যাংক/শাখা বা এনবিএফআই 'শেষ নিরীক্ষা রিপোর্টে' (বাহ্যিক/অভ্যন্তরীণ) করা সুপারিশগুলো মোকাবেলার জন্য যথাযথ ব্যবস্থা গ্রহণ করবে। এটি অবশ্যই নথিভুক্ত করতে হবে।

### ৫.২.৫ বাহ্যিক ইনফরমেশন সিস্টেম নিরীক্ষা (External Information System Audit)

i) ব্যাংক বা NBFI তাদের নিয়মিত আর্থিক নিরীক্ষার অডিট করার পাশাপাশি তাদের তথ্য সিস্টেমের জন্য বহিরাগত নিরীক্ষককে নিযুক্ত করতে পারে।

ii) নিরীক্ষা রিপোর্ট নিয়ন্ত্রকদের জন্য সংরক্ষণ করা হবে এবং যখন প্রয়োজন হবে তখন তা দেখাতে হবে।

### ৫.২.৬ স্ট্যান্ডার্ড সার্টিফিকেশন (Standard Certification)

ব্যাংক বা এনবিএফআই তাদের ইনফরমেশন সিস্টেম নিরাপত্তা, আইসিটি পরিষেবা সরবরাহের গুণমান, ব্যবসার ধারাবাহিকতা ব্যবস্থাপনা, পেমেন্ট কার্ড ডেটা নিরাপত্তা, ইত্যাদি সম্পর্কিত ইন্ডাস্ট্রি স্ট্যান্ডার্ড সার্টিফিকেশন পেতে পারে।

### ৫.২.৭ নিরাপত্তা সচেতনতা এবং প্রশিক্ষণ

i) প্রযুক্তির দ্রুত বিকাশের সঙ্গে সঙ্গে, ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে সমস্ত প্রাসঙ্গিক কর্মীরা তাদের কাজের ওপর প্রশিক্ষণের পাশাপাশি আইসিটি নিরাপত্তা কার্যক্রমের ওপরও যথাযথ প্রশিক্ষণ, শিক্ষা ও সচেতনতা পাচ্ছে।

ii) ব্যাংক বা এনবিএফআই আইসিটি কর্মীদের জন্য বিজনেস ফাউন্ডেশন প্রশিক্ষণের ন্যূনতম স্তর নিশ্চিত করবে।

iii) ব্যাংক বা এনবিএফআই সমস্ত কর্মীদের জন্য নিরাপত্তা সচেতনতা প্রশিক্ষণ/ওয়ার্কশপের ব্যবস্থা করবে।

iv) ব্যাংক বা এনবিএফআই কোনো নতুন ব্যাংকিং পরিষেবা এবং প্রযুক্তিগত পরিবর্তন বিবেচনা করে IS অডিট দলের জন্য পর্যাপ্ত প্রশিক্ষণ প্রদান করবে।

### ৫.২.৮ বীমা বা ঝুঁকি কভারেজ তহবিল

i) পর্যাপ্ত বীমা কভারেজ বা ঝুঁকি কভারেজ তহবিল রক্ষণাবেক্ষণ করা হবে যাতে আইসিটি সম্পদের ক্ষতি কমানো যায়।

ii) ব্যাংক বা এনবিএফআই-এর অ্যাকাউন্টিং সিস্টেমে ঝুঁকি কভারেজ তহবিল যথাযথভাবে রক্ষণাবেক্ষণ করতে হবে (যদি প্রযোজ্য হয়)।

iii) প্রয়োজনে ঝুঁকি কভারেজ তহবিল ব্যবহার করার জন্য একটি স্পষ্ট নীতিমালা থাকতে হবে (যদি এটি বজায় থাকে)।

## ৫.৩. আইসিটি ঝুঁকি ব্যবস্থাপনা (ICT Risk Management)

আইসিটি ঝুঁকি হলো একটি এন্টারপ্রাইজের সামগ্রিক ঝুঁকির একটি অংশ। ব্যাংক বা এনবিএফআই-এর অন্যান্য ঝুঁকির মধ্যে রয়েছে কৌশলগত ঝুঁকি, পরিবেশগত ঝুঁকি, বাজারের ঝুঁকি, ক্রেডিট ঝুঁকি, অপারেশনাল ঝুঁকি, কমপ্লায়েন্স ঝুঁকি, ইত্যাদি। অনেক প্রতিষ্ঠানে আইসিটি সম্পর্কিত ঝুঁকিকে অপারেশনাল ঝুঁকির একটি অংশ হিসেবে বিবেচনা করা হয়।

এমনকি কৌশলগত ঝুঁকিরও একটি আইসিটি উপাদান থাকতে পারে, বিশেষ করে যেখানে আইসিটি নতুন ব্যবসায়িক উদ্যোগের মূল চালিকাশক্তি। ক্রেডিট ঝুঁকির ক্ষেত্রেও একই কথা প্রযোজ্য, দুর্বল আইসিটি নিরাপত্তার কারণে ক্রেডিট রেটিং কম হতে পারে। আইসিটি ঝুঁকিকে অন্যান্য ঝুঁকির ওপর নির্ভরশীল হিসাবে না দেখাই ভালো।

আইসিটি ঝুঁকি হলো ব্যবসায়িক ঝুঁকি-বিশেষত, ব্যাংক বা এনবিএফআই-এর মধ্যে আইসিটি ব্যবহার, মালিকানা, পরিচালনা, প্রভাব এবং গ্রহন সংক্রান্ত ব্যবসায়িক ঝুঁকি। এতে আইসিটি সম্পর্কিত ইভেন্ট এবং শর্ত রয়েছে, যা ব্যবসায়িকভাবে প্রভাব ফেলতে পারে। এটি অনিশ্চিত ফ্রিকোয়েন্সি এবং বিশালতায় সংঘটিত হতে পারে এবং এটি কৌশলগত লক্ষ্য এবং উদ্দেশ্য পূরণে চ্যালেঞ্জ তৈরি করে।

### ৫.৩.১ আইসিটি ঝুঁকি নিয়ন্ত্রণ (ICT Risk Governance)

i) ব্যাংক বা এনবিএফআই সামগ্রিক আইসিটি ঝুঁকি এবং প্রাসঙ্গিক নিরাপত্তা ব্যবস্থা পরিচালনা করার জন্য একটি আইসিটি ঝুঁকি ব্যবস্থাপনা কমিটি গঠন করবে।

ii) ব্যাংক বা এনবিএফআই ঝুঁকির এপিটাইট (ঝুঁকির পরিমাণ ব্যাংক বা এনবিএফআই তার উদ্দেশ্যগুলো অর্জনের জন্য গ্রহণ করতে প্রস্তুত) সম্ভাব্য

ক্ষতি গ্রহণের ঝুঁকির ফ্রিকোয়েন্সি এবং মাত্রা যেমন, আর্থিক ক্ষতি, সুনামের ক্ষতি ইত্যাদির সংমিশ্রণে সংজ্ঞায়িত করবে।

iii) ব্যাংক বা এনবিএফআই বোর্ড/ঝুঁকি ব্যবস্থাপনা কমিটির অনুমোদন নিয়ে ঝুঁকি সহনশীলতা (ঝুঁকি এপিটাইট সংজ্ঞা দ্বারা নির্ধারিত স্তর থেকে সহনীয় বিচ্যুতি) সংজ্ঞায়িত করবে এবং সমস্ত স্টেকহোল্ডারদের কাছে স্পষ্টভাবে জানাবে।

iv) ব্যাংক বা এনবিএফআই সময়ের সঙ্গে ঝুঁকির এপিটাইট এবং সহনশীলতার পরিবর্তন পর্যালোচনা এবং অনুমোদন করবে; বিশেষত নতুন প্রযুক্তি, নতুন সাংগঠনিক কাঠামো, নতুন ব্যবসায়িক কৌশল এবং অন্যান্য কারণগুলোর জন্য এন্টারপ্রাইজকে নিয়মিত বিরতিতে তার ঝুঁকি পোর্টফোলিও পুনর্মূল্যায়ন করবে।

v) ব্যাংক বা এনবিএফআই ব্যক্তিদের দায়িত্ব সফলভাবে সমাপ্তি নিশ্চিত করার জন্য প্রত্যেকের ঝুঁকির পরিমান নির্ধারণ করবে।

vi) ব্যাংক বা এনবিএফআই তাদের প্রত্যেকের ঝুঁকির জবাবদিহিতাকে সংজ্ঞায়িত করবে, যারা প্রয়োজনীয় সংস্থানগুলোর মালিক এবং যাদের কাছে নির্দিষ্ট আইসিটি ঝুঁকি প্রক্রিয়ার মধ্যে কোনো কার্যকলাপের ফলাফলকে কার্যকর করার অথবা গ্রহণ করার ক্ষমতা রয়েছে। ঝুঁকির মালিকানা নির্দিষ্ট আইসিটি সম্পদের জন্য চিহ্নিত ঝুঁকি প্রশমিত করার জন্য দায়ি ব্যক্তিদের কাছেই থাকে।

vii) ব্যাংক বা এনবিএফআই ঝুঁকি সচেতনতার মাধ্যমে সমস্ত ঝুঁকি স্বীকার করবে যাতে সেগুলো ভালভাবে বোঝা ও জানা যায় এবং সেগুলো পরিচালনা করার উপায় হিসাবে স্বীকৃত হয়।

viii) ব্যাংক বা এনবিএফআই ওপেন কমিউনিকেশনের মাধ্যমে উপযুক্ত এবং অবহিত ঝুঁকি প্রতিক্রিয়াগুলোর সংজ্ঞা সক্ষম করে আইসিটি ঝুঁকির প্রকৃত এক্সপোজার সম্পর্কে নির্বাহী ব্যবস্থাপনা বোঝার জন্য অবদান রাখবে।

ix) ব্যাংক বা এনবিএফআই সমস্ত অভ্যন্তরীণ স্টেকহোল্ডারদেরকে তাদের দৈনন্দিন দায়িত্বে ঝুঁকি ও সুযোগকে একীভূত করার গুরুত্ব সম্পর্কে সচেতন করবে।

x) ব্যাংক বা এনবিএফআই বহিরাগত স্টেকহোল্ডারদের কাছে প্রকৃত ঝুঁকি এবং ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া সম্পর্কে স্বচ্ছ থাকবে।

xi) ব্যাংক বা এনবিএফআই বোর্ড ও এক্সিকিউটিভ, যারা দিকনির্দেশনা নির্ধারণ করে, ঝুঁকি-সচেতন সিদ্ধান্ত গ্রহণে যোগাযোগ করে এবং কার্যকর ঝুঁকি ব্যবস্থাপনা আচরণকে পুরস্কৃত করে, এমন শীর্ষ থেকে ঝুঁকি সচেতন সংস্কৃতি শুরু করবে।

xii) আইসিটি সিকিউরিটি ডিপার্টমেন্ট/ইউনিট/সেল আইসিটি সিকিউরিটি কমিটি এবং ঝুঁকি ব্যবস্থাপনা কমিটির কাছে আইসিটি সিকিউরিটি রিস্কের স্ট্যাটাস রিপোর্ট করবে যা নীতিমালায় সংজ্ঞায়িত করা হবে।

### ৫.৩.২. আইসিটি ঝুঁকি মূল্যায়ন (ICT Risk Assesment)

অর্থপূর্ণ আইসিটি ঝুঁকি মূল্যায়ন ও ঝুঁকিভিত্তিক সিদ্ধান্তের জন্য আইসিটি ঝুঁকিগুলোকে দ্ব্যর্থহীন এবং স্পষ্ট, ব্যবসা-প্রাসঙ্গিক শর্তে প্রকাশ করা প্রয়োজন। কার্যকর ঝুঁকি ব্যবস্থাপনার জন্য আইসিটি এবং ব্যবসার মধ্যে পারস্পরিক বোঝাপড়া প্রয়োজন, যার ওপর ঝুঁকি পরিচালনা করা দরকার। সব স্টেকহোল্ডারের অবশ্যই বোঝা ও প্রকাশ করার ক্ষমতা থাকতে হবে যে কীভাবে প্রতিকূল ঘটনাগুলো ব্যবসার উদ্দেশ্যগুলোকে প্রভাবিত করতে পারে। একজন আইসিটি ব্যক্তি বুঝতে পারবেন যে কীভাবে আইসিটি-সম্পর্কিত ব্যর্থতা বা ঘটনাগুলো এন্টারপ্রাইজের উদ্দেশ্যগুলোকে প্রভাবিত করতে পারে এবং এন্টারপ্রাইজের প্রত্যক্ষ বা পরোক্ষ ক্ষতির কারণ হতে পারে। আইসিটি-সম্পর্কিত ব্যর্থতা বা ঘটনাগুলো কীভাবে মূল পরিষেবা এবং প্রক্রিয়াগুলোকে প্রভাবিত করতে পারে তা একজন ব্যবসায়ী ব্যক্তি বুঝতে পারবেন।

i) ব্যাংক বা এনবিএফআই প্রতিকূল ঘটনাগুলোর ব্যবসায়িক প্রভাব বিশ্লেষণের প্রয়োজন রয়েছে। ব্যাংক বা NBFI বিভিন্ন কৌশল ও বিকল্পগুলো অনুশীলন করতে পারে, যা তাদের ব্যবসায়িক পরিভাষায় আইসিটি ঝুঁকি বর্ণনা করতে সাহায্য করবে।

ii) ব্যাংক বা এনবিএফআই সবচেয়ে গুরুত্বপূর্ণ এবং প্রাসঙ্গিক ঝুঁকিগুলো চিহ্নিত করার জন্য, ঝুঁকি পরিস্থিতি কৌশল তৈরি ও ব্যবহার অনুশীলন করবে। যেখানে ঝুঁকির ফ্রিকোয়েন্সি ও প্রভাব মূল্যায়ন করা হয় সেখানে তৈরি ঝুঁকির পরিস্থিতি সমূহ বিভিন্ন ঝুঁকি বিশ্লেষণের সময় ব্যবহার করা যেতে পারে।

iii) ব্যাংক বা এনবিএফআই ঝুঁকির কারণগুলোকে সংজ্ঞায়িত করবে যেগুলো ঝুঁকির পরিস্থিতির ফ্রিকোয়েন্সি অথবা ব্যবসায়িক প্রভাবকে প্রভাবিত করে।

iv) ব্যাংক বা এনবিএফআই ঝুঁকির কারণগুলোকে বাস্তবায়িত পরিস্থিতির নৈমিত্তিক কারণ হিসাবে বা দুর্বলতা হিসাবে ব্যাখ্যা করবে।

v) আইসিটি নিরাপত্তা বিভাগ/ইউনিট/সেল আইসিটি সম্পর্কিত সম্পদের (প্রক্রিয়া এবং সিস্টেম) পর্যায়ক্রমিক আইসিটি ঝুঁকি মূল্যায়ন পরিচালনা করবে এবং ঝুঁকি কমানোর জন্য মালিকদের সুপারিশ প্রদান করবে।

### ৫.৩.৩ আইসিটি ঝুঁকি প্রতিক্রিয়া (ICT Risk Response)

ঝুঁকি প্রতিক্রিয়া হলো সংস্থার জন্য সংজ্ঞায়িত ঝুঁকি সহনশীলতার স্তরের সঙ্গে মিলিয়ে ঝুঁকি কমিয়ে আনা। অন্য কথায়, একটি প্রতিক্রিয়া এমনভাবে সংজ্ঞায়িত করা দরকার যে যতটা সম্ভব ভবিষ্যতের অবশিষ্ট ঝুঁকি (সাধারণত সহজলভ্য বাজেটের ওপর নির্ভর করে) সহনশীলতার সীমার মধ্যে পড়ে। যখন বিশ্লেষণে সংজ্ঞায়িত সহনশীলতার মাত্রা থেকে বিচ্যুত হওয়ার ঝুঁকি দেখায়, তখন একটি প্রতিক্রিয়া সংজ্ঞায়িত করা প্রয়োজন। এই প্রতিক্রিয়া চারটি সম্ভাব্য উপায় যেমন ঝুঁকি পরিহার, ঝুঁকি হ্রাস/প্রশমন, ঝুঁকি ভাগাভাগি/স্থানান্তর এবং ঝুঁকি গ্রহণযোগ্যতার যেকোনো একটি হতে পারে।

i) ব্যাংক বা এনবিএফআই ঝুঁকি সূচক হিসাবে কাজ করার জন্য মেট্রিক্সের একটি সেট তৈরি করবে। উচ্চ ব্যবসায়িক প্রভাবসহ ঝুঁকির জন্য সূচকগুলো সম্ভবত মূল ঝুঁকি নির্দেশক (KRIs) হবে।

ii) সংবেদনশীলতার সমতুল্য বিভিন্ন সূচক বাস্তবায়ন, পরিমাপ এবং রিপোর্ট করার জন্য ব্যাংক বা এনবিএফআই প্রচেষ্টা চালাবে।

iii) ব্যাংক বা এনবিএফআই- KRIs এর সঠিক সেট নির্বাচন করার উদ্দেশ্যে নিম্নলিখিতগুলো বাস্তবায়ন করবে।

ক) সক্রিয় পদক্ষেপ নেওয়ার জন্য উচ্চ ঝুঁকির একটি প্রাথমিক সতর্কতা প্রদান করা।

খ) ঘটে যাওয়া ঝুঁকিপূর্ণ ঘটনাগুলোর ওপর একটি পশ্চাৎমুখী দৃষ্টিভঙ্গি প্রদান করা।

গ) প্রবণতাগুলোর ডকুমেন্টেশন এবং বিশ্লেষণ সক্ষম করা।

ঘ) মেট্রিক সেটিংয়ের মাধ্যমে ঝুঁকির এপিটাইট এবং সহনশীলতার একটি ইঙ্গিত প্রদান করা।

ঙ) কৌশলগত উদ্দেশ্য অর্জনের সম্ভাবনা বৃদ্ধি করা।

চ) ঝুঁকি শাসন ও ব্যবস্থাপনা পরিবেশ ক্রমাগত অপ্টিমাইজ করতে সহায়তা করা।

iv) ব্যাংক বা এনবিএফআই ঝুঁকি বিশ্লেষণের পরে ব্যাংক বা এনবিএফআই-এর সংজ্ঞায়িত ঝুঁকির এপিটাইট অনুসারে ঝুঁকির প্রতিক্রিয়া সংজ্ঞায়িত করবে।

v) ব্যাংক বা এনবিএফআই ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার সঙ্গে সামগ্রিক আইসিটি ঝুঁকি ব্যবস্থাপনা অনুশীলনকে শক্তিশালী করবে।

vi) ব্যাংক বা এনবিএফআই কোনো প্রতিকূল ঘটনা অথবা কোনো ইভেন্টের ব্যবসায়িক প্রভাবকে হ্রাস করার উদ্দেশ্যে বেশ কয়েকটি নিয়ন্ত্রণ ব্যবস্থা প্রবর্তন করবে।

vii) ব্যাংক বা এনবিএফআই ঝুঁকির একটি অংশ স্থানান্তর বা অন্যথায় ভাগ করে ঝুঁকির ফ্রিকোয়েন্সি বা প্রভাবকে হ্রাস করবে, যেমন বীমা, আউটসোর্সিংয়ের মাধ্যমে।

## ৫.৪. আইসিটি সার্ভিস ডেলিভারি ব্যবস্থাপনা (ICT Service Delivery Management)

আইসিটি সার্ভিস ম্যানেজমেন্ট, অপারেশন ম্যানেজমেন্টের প্রযুক্তি কভার করে, যার মধ্যে রয়েছে ক্ষমতা ব্যবস্থাপনা (capacity management), অনুরোধ ব্যবস্থাপনা (request management), পরিবর্তন ব্যবস্থাপনা, ঘটনা এবং সমস্যা ব্যবস্থাপনা, ইত্যাদি। উদ্দেশ্য হলো ন্যূনতম অপারেশনাল ঝুঁকির মাধ্যমে আইসিটি পরিষেবার গুণমানের সর্বোচ্চ স্তর অর্জনের জন্য নিয়ন্ত্রণ সেট করা।

### ৫.৪.১ পরিবর্তন ব্যবস্থাপনা (Change Management)

i) তথ্য প্রক্রিয়াকরণ সুবিধা এবং সিস্টেমের পরিবর্তনগুলো নিয়ন্ত্রণ করা।

ii) ব্যাংক বা এনবিএফআই 'ব্যবসায়িক প্রয়োজনীয় দলিল' (বিআরডি) প্রস্তুত করবে যা সিস্টেম পরিবর্তনের প্রয়োজনীয়তা এবং ব্যবসায়িক প্রক্রিয়া, নিরাপত্তা ম্যাট্রিক্স, রিপোর্টিং, ইন্টারফেস, ইত্যাদি বর্ননা করবে।

iii) উৎপাদন পরিবেশে বাস্তবায়িত ব্যবসায়িক প্রয়োগের সমস্ত পরিবর্তনগুলো প্রয়োজনীয় পরিবর্তনের বিবরণসহ একটি আনুষ্ঠানিক নথিভুক্ত প্রক্রিয়া দ্বারা নিয়ন্ত্রিত করা।

iv) ব্যবসায়িক অ্যাপ্লিকেশনের জন্য অডিট পদ্ধতি বজায় রাখা।

v) ব্যাংক বা এনবিএফআই অপ্রত্যাশিত পরিস্থিতির জন্য রোল-ব্যাক প্ল্যান তৈরি করা।

vi) অ্যাপ্লিকেশনে স্থাপনের পূর্বে সব পরিবর্তন ও হালনাগাদের ওপর ইউজার একসেপ্টেন্স টেস্ট (UAT) করা।

vii) স্থাপনের পর ইউজার ভ্যারিফিকেশন টেস্ট (UVT) করা।

**৫.৪.২ ঘটনা ব্যবস্থাপনা (Incident Management)**

একটি ঘটনা সংঘটিত হয় তখনই যখন আইসিটি পরিষেবা সরবরাহের মানে একটি অপ্রত্যাশিত ব্যাঘাত ঘটে। ব্যাংক বা এনবিএফআই এই ধরনের ঘটনাগুলো যথাযথভাবে পরিচালনা করবে, যাতে আইসিটি পরিষেবার দীর্ঘস্থায়ী ব্যাঘাত ঘটতে পারে এমন ভুল ব্যবস্থাপনার পরিস্থিতি এড়ানো যায়।

i) ব্যাংক বা এনবিএফআই ব্যবসায়িক ক্রিয়াকলাপগুলোতে ন্যূনতম প্রভাবসহ ঘটনার পর যত তাড়াতাড়ি সম্ভব স্বাভাবিক আইসিটি পরিষেবা পুনরুদ্ধারের লক্ষ্যে একটি ঘটনা ব্যবস্থাপনা কাঠামো (incident management framework) স্থাপন করবে। ব্যাংক বা এনবিএফআই ঘটনা ব্যবস্থাপনা প্রক্রিয়ার সঙ্গে জড়িত কর্মীদের ভূমিকা ও দায়িত্বও স্থাপন করবে, যার মধ্যে ঘটনাগুলো রেকর্ডিং, বিশ্লেষণ, প্রতিকার এবং পর্যবেক্ষণ অন্তর্ভুক্ত রয়েছে।

ii) এটি গুরুত্বপূর্ণ যে ঘটনাগুলোকে যথাযথ তীব্রতার স্তরে ভাগ করা হয়। ঘটনা বিশ্লেষণের অংশ হিসাবে, ব্যাংক বা NBFI একটি প্রযুক্তিগত হেল্পডেস্ক-কে ঘটনার তীব্রতা মাত্রা নির্ধারণ ও বরাদ্দ করার দায়িত্ব দিতে পারে। ব্যাংক বা এনবিএফআই হেল্পডেস্কের কর্মীদের উচ্চ তীব্রতার স্তরের ঘটনাগুলো নির্ধারণ করতে প্রশিক্ষিত করবে। উপরন্তু, ঘটনার তীব্রতা স্তরের মূল্যায়নের জন্য ব্যবহৃত মানদণ্ড প্রতিষ্ঠিত এবং নথিভুক্ত করতে হবে।

iii) ব্যাংক বা এনবিএফআই সংশ্লিষ্ট escalation and resoluting পদ্ধতি স্থাপন করবে যেখানে রেজোলিউশনের সময়সীমা ঘটনার তীব্রতার স্তরের সঙ্গে সমানুপাতিক হবে।

iv) নিরাপত্তা ঘটনার জন্য পূর্বনির্ধারিত escalation and response পরিকল্পনা পর্যায়ক্রমিক ভিত্তিতে পরীক্ষা করতে হবে।

v) ব্যাংক বা এনবিএফআই একটি আইসিটি ইমার্জেন্সি রেসপন্স টিম গঠন করবে, যার মধ্যে ব্যাংক বা এনবিএফআই-এর কারিগরি ও অপারেশনাল দক্ষতা সম্পন্ন কর্মীরা থাকবে, যাতে বড় ধরনের ঘটনাগুলো মোকাবেলা করা যায়।

vi) কিছু পরিস্থিতিতে, বড় ঘটনা আরও প্রতিকূলভাবে সংকটে পরিণত হতে পারে। ঊর্ধ্বতন ব্যবস্থাপনাকে এই ঘটনা সম্পর্কে অবহিত করতে হবে যাতে দুর্যোগ পুনরুদ্ধার পরিকল্পনা সক্রিয় করার সিদ্ধান্ত সময়মতো নেওয়া যায়। ব্যাংক বা এনবিএফআই যত তাড়াতাড়ি সম্ভব বাংলাদেশ ব্যাংককে জানাবে যে তার দুর্যোগ পুনরুদ্ধার ব্যবস্থায় ব্যর্থ হয়েছে।

vii) ব্যাংক বা এনবিএফআই গ্রাহকদের যে কোনো বড় ঘটনা সম্পর্কে অবহিত করবে। একটি সংকট বা জরুরি পরিস্থিতিতে গ্রাহকের আস্থা বজায় রাখতে পারা ব্যাংক বা এনবিএফআই এর সুনামের জন্য অত্যন্ত গুরুত্বপূর্ণ।

viii) যেহেতু ঘটনাগুলো অনেক কারণে হতে পারে, তাই ব্যাংক বা এনবিএফআই প্রধান ঘটনাগুলোর মূল কারণ এবং প্রভাব বিশ্লেষণ করবে। ব্যাংক বা এনবিএফআই অনুরূপ ঘটনার পুনরাবৃত্তি রোধ করতে প্রতিকারমূলক ব্যবস্থা গ্রহণ করবে।

ix) মূল কারণ এবং প্রভাব বিশ্লেষণ প্রতিবেদনে নিম্নলিখিত ক্ষেত্রগুলোকে অন্তর্ভুক্ত করতে হবে

**ক) মূল কারণ বিশ্লেষণ (Root cause analysis)**

i. কখন এটা ঘটেছিল?
ii. এটা কোথায় ঘটেছে?
iii. ঘটনাটি কেন এবং কীভাবে ঘটল?
iv. গত ২ বছরে কতবার অনুরূপ ঘটনা ঘটেছে?
v. এই ঘটনা থেকে কি শিক্ষা নেওয়া হয়েছে?

**খ) প্রভাব বিশ্লেষণ (Impact Analysis)**

i. সিস্টেম, সম্পদ এবং ক্ষতিগ্রস্ত গ্রাহকদের তথ্যসহ ঘটনার ব্যাপ্তি;
ii. হারানো রাজস্ব, ক্ষতি, খরচ, বিনিয়োগ, ক্ষতিগ্রস্ত গ্রাহকের সংখ্যা, প্রভাব, সুনাম এবং আত্মবিশ্বাসের পরিণতিসহ ঘটনার মাত্রা;
iii. ঘটনার ফলে নিয়ন্ত্রকের যে সমস্ত প্রয়োজনীয়তা এবং শর্তাবলি লঙ্ঘন হয়েছে।

**গ) সংশোধনমূলক এবং প্রতিরোধমূলক ব্যবস্থা (Corrective and Preventive measures)**

i. ঘটনার পরিণতি মোকাবেলায় অবিলম্বে সংশোধনমূলক ব্যবস্থা নেওয়া হবে। গ্রাহকদের উদ্বেগের বিষয়ে অগ্রাধিকার দিতে হবে।
ii. ঘটনার মূল কারণ খুঁজে বের করার ব্যবস্থা করা।
iii. অনুরূপ ঘটনার পুনরাবৃত্তি যাতে না ঘটে তার ব্যবস্থা নেওয়া।

**৫.৪.১ সমস্যা ব্যবস্থাপনা (Problem Managament)**

ঘটনা ব্যবস্থাপনার (Incident Management) উদ্দেশ্য হলো যত তাড়াতাড়ি সম্ভব আইসিটি পরিষেবা পুনরুদ্ধার করা আর সমস্যা ব্যবস্থাপনার (Problem

Managament) লক্ষ্য হলো মূল কারণ নির্ণয় করা এবং নির্মূল করা যাতে বারবার ঘটনার সংঘটন রোধ করা যায়।

i) ব্যাংক বা NIFI তথ্য সিস্টেম-সম্পর্কিত সমস্যাগুলো লগ করার জন্য একটি প্রক্রিয়া স্থাপন করবে।

ii) দ্রুত, কার্যকরী এবং সুশৃঙ্খল প্রতিক্রিয়া (response) পেতে একজন ঊর্ধ্বতন ব্যক্তির কাছে কোনো সমস্যা escalate করার উদ্দেশ্যে ব্যাংক বা NBFI-এর কাছে কর্মপ্রবাহের প্রক্রিয়া (Process of workflow) থাকবে।

iii) সমস্যা-সমাধান প্রক্রিয়া চলাকালীন সময়ে সমস্যা চিহ্নিতকরণ এবং গৃহীত পদক্ষেপগুলো নথিভুক্ত করতে হবে।

iv) অনুরূপ সমস্যাসমূহ শনাক্তকরণ এবং প্রতিরোধের সুবিধার্থে অতীতের সমস্যাগুলোর একটি প্রবণতা বিশ্লেষণ (trend analysis) করতে হবে।

### ৫.৪.৪ সক্ষমতা ব্যবস্থাপনা (Capacity Management)

সক্ষমতা ব্যবস্থাপনার লক্ষ্য হলো আইসিটি সক্ষমতা বর্তমান এবং ভবিষ্যতের ব্যবসায়িক প্রয়োজনীয়তাগুলোকে যেন সাশ্রয়ী পদ্ধতিতে পূরণ করে, তা নিশ্চিত করা।

i) আইসিটি সিস্টেম এবং পরিকাঠামো ব্যবসায়িক কার্যাবলিকে সমর্থন করতে সক্ষম তা নিশ্চিত করার জন্য, ব্যাংক বা NBFI কর্মক্ষমতা, স্বক্ষমতা এবং ব্যবহারের মতো সূচকগুলো পর্যবেক্ষণ ও পর্যালোচনা করবে।

ii) ব্যাংক বা এনবিএফআই নিরীক্ষণ প্রক্রিয়াগুলো স্থাপন করবে এবং কার্যকরভাবে কার্যকরী এবং ব্যবসায়ের প্রয়োজনীয়তা পূরণের জন্য অতিরিক্ত সংস্থান পরিকল্পনা ও নির্ধারণের জন্য উপযুক্ত থ্রেশহোল্ড বাস্তবায়ন করবে।

## ৫.৫. অবকাঠামো নিরাপত্তা ব্যবস্থাপনা (Infrastructure Security Management )

আইসিটি ল্যান্ডস্কেপ বিভিন্ন ধরনের আক্রমণের জন্য ঝুঁকিপূর্ণ। এই ধরনের আক্রমণের ফ্রিকোয়েন্সি ও ম্যালিগন্যান্সি বাড়ছে। এটি অপরিহার্য যে ব্যাংক বা NBFI ডেটা, অ্যাপ্লিকেশন, ডাটাবেস, অপারেটিং সিস্টেম এবং নেটওয়ার্কগুলোতে পর্যাপ্তভাবে সম্পর্কিত হুমকিগুলো মোকাবেলা করার জন্য সুরক্ষা সমাধানগুলো প্রয়োগ করে। সংবেদনশীল বা গোপনীয় তথ্য যেমন গ্রাহকের ব্যক্তিগত তথ্য এবং সিস্টেমে সংরক্ষিত এবং প্রক্রিয়াজাত করা অ্যাকাউন্ট এবং লেনদেনের ডেটা সুরক্ষার জন্য উপযুক্ত ব্যবস্থা প্রয়োগ করা হয়। অনলাইন লেনদেন এবং সংবেদনশীল ব্যক্তিগত বা অ্যাকাউন্ট তথ্য অ্যাক্সেস করার আগে গ্রাহকদের সঠিকভাবে অথেনটিকেট্ করা হয়।

### ৫.৫.১ সম্পদ ব্যবস্থাপনা (Asset Management)

i) কোনো নতুন আইসিটি সম্পদ সংগ্রহ করার আগে, ব্যাংক বা এনবিএফআই দ্বারা (বিদ্যমান সিস্টেমের সঙ্গে) সামঞ্জস্য মূল্যায়ন (Compatibiltiy Assesment) করা হবে।

ii) সমস্ত আইসিটি সম্পদ সংগ্রহের ক্ষেত্রে ব্যাংক বা এনবিএফআই-এর ক্রয় নীতি মেনে চলতে হবে।

ii) প্রতিটি আইসিটি সম্পদ একজন অভিভাবককের (একজন ব্যক্তি বা সত্তা) কাছে বরাদ্দ করা হবে যিনি সেই সম্পদের উন্নয়ন, রক্ষণাবেক্ষণ, ব্যবহার, নিরাপত্তা এবং অখণ্ডতার জন্য দায়ী থাকবেন।

iv) সমস্ত আইসিটি সম্পদ স্পষ্টভাবে চিহ্নিত এবং লেবেল করা হবে। লেবেলিং সম্পদের প্রতিষ্ঠিত শ্রেণিবিন্যাস প্রতিফলিত করবে।

v) ব্যাংক বা এনবিএফআই একটি আইসিটি সম্পদ ইনভেন্টরি বজায় রাখবে যাতে উল্লেখযোগ্য বিশদ বিবরণ থাকে (যেমন মালিক, অভিভাবক, ক্রয়ের তারিখ, অবস্থান, লাইসেন্স নম্বর, কনফিগারেশন ইত্যাদি)।

vi) ব্যাংক বা এনবিএফআই পর্যায়ক্রমে আইসিটি সম্পদের তালিকা পর্যালোচনা ও হালনাগাদ করবে।

vii) ইনফরমেশন সিস্টেমের সম্পদগুলো অননুমোদিত অ্যাক্সেস, অপব্যবহার, বা জালিয়াতিপূর্ণ পরিবর্তন, সন্নিবেশ, মুছে ফেলা, প্রতিস্থাপন, দমন, বা প্রকাশ থেকে পর্যাপ্তভাবে সুরক্ষিত থাকবে।

viii) ব্যাংক বা এনবিএফআই ইনফরমেশন সিস্টেম সম্পদ সুরক্ষার জন্য একটি নিষ্পত্তি নীতি প্রতিষ্ঠা করবে। বিক্রয়, নিষ্পত্তি বা পুনরায় ইস্যু করার আগে সরঞ্জাম এবং সংশ্লিষ্ট স্টোরেজ মিডিয়ার সমস্ত ডেটা অবশ্যই ধ্বংস বা ওভাররাইট করতে হবে।

ix) ব্যাংক বা এনবিএফআই পোর্টেবল ডিভাইসের ব্যবহারের জন্য নির্দেশিকা প্রদান করবে, বিশেষ করে ব্যাংক বা এনবিএফআইয়ের বাইরে ব্যবহারের জন্য।

x) ব্যাংক বা এনবিএফআই তাদের কর্মসংস্থান, চুক্তি বা চুক্তির সমাপ্তির পরে কর্মচারী/বহিরাগত পক্ষের কাছ থেকে সাংগঠনিক সম্পদ ফেরত নেওয়ার নীতি তৈরি করবে।

xi) ব্যাংক বা এনবিএফআই সমস্ত সফ্টওয়্যার লাইসেন্সের শর্তাবলি মেনে চলবে এবং এমন কোনো সফ্টওয়্যার ব্যবহার করবে না, যা আইনত ক্রয় করা হয়নি বা অন্যথায় বৈধভাবে প্রাপ্ত করা হয়নি।

xii) উৎপাদন পরিবেশে ব্যবহৃত আউটসোর্সড সফ্টওয়্যার, বিক্রেতার সঙ্গে সাপোর্ট চুক্তির অধীন থাকবে।

xiii) ব্যাংক বা এনবিএফআই সফ্টওয়্যারের তালিকা অনুমোদন করবে যা যে কোনো কম্পিউটারে ব্যবহার করা যাবে।

xiv) ব্যাংক বা এনবিএফআই জুড়ে অননুমোদিত বা পাইরেটেড সফ্টওয়্যার ব্যবহার কঠোরভাবে নিষিদ্ধ করা হবে।

### ৫.৫.২. ডেস্কটপ/ল্যাপটপ ডিভাইস নিয়ন্ত্রণ (Desktop/Laptop Device Controls)

i) ডেটা এবং হার্ডওয়্যারের ক্ষতি রোধ করতে ডেস্কটপ কম্পিউটারগুলো ইউপিএস-এর সঙ্গে সংযুক্ত থাকতে হবে।

ii) একটি ডেস্কটপ বা ল্যাপটপ কম্পিউটারকে অনুপস্থিত (unattended) রেখে যাওয়ার আগে, ব্যবহারকারীদের 'লক ওয়ার্কস্টেশন' বৈশিষ্ট্যটি প্রয়োগ করতে হবে। প্রয়োগ না করা হলে ব্যাংক বা NBFI-এর নীতি অনুযায়ী ডিভাইসটি স্বয়ংক্রিয়ভাবে লক হয়ে যাবে।

iii) ল্যাপটপে সংরক্ষিত গোপনীয় বা সংবেদনশীল তথ্য এনক্রিপ্ট করা থাকবে।

iv) প্রতিটি কর্মদিবসের শেষে ডেস্কটপ কম্পিউটার, ল্যাপটপ, মনিটর ইত্যাদি বন্ধ করে দেওয়া হবে।

v) ল্যাপটপ, কম্পিউটার মিডিয়া এবং সংবেদনশীল তথ্য ধারণকারী অপসারণযোগ্য স্টোরেজের অন্য যেকোনো ফর্ম (যেমন-সিডি, রম, জিপ ডিস্ক, পিডিএ, ফ্ল্যাশ ড্রাইভ, বাহ্যিক হার্ড ড্রাইভ) যখন ব্যবহার করা হবে না তখন একটি সুরক্ষিত স্থানে বা লক করা ক্যাবিনেটে সংরক্ষণ করা হবে।

vi) ডেস্কটপ/ল্যাপটপ কম্পিউটারের জন্য ইউএসবি পোর্টের অ্যাক্সেস নিয়ন্ত্রণ করা হবে।

vii) গোপনীয় তথ্য ধারণকারী অন্যান্য তথ্য স্টোরেজ মিডিয়া যেমন কাগজ, ফাইল, টেপ ইত্যাদি ব্যবহার না করার সময় একটি সুরক্ষিত স্থানে বা লক করা ক্যাবিনেটে সংরক্ষণ করা হবে।

viii) পূর্ব অনুমোদন ছাড়াই স্বতন্ত্র ব্যবহারকারীদের দ্বারা সফ্টওয়্যার অ্যাপ্লিকেশন এবং/অথবা এক্সিকিউটেবল ফাইল যেকোনো ডেস্কটপ বা ল্যাপটপ কম্পিউটারে ইনস্টল বা ডাউনলোড করা যাবে না।

ix) ডেস্কটপ এবং ল্যাপটপ কম্পিউটার ব্যবহারকারীরা জ্ঞাতসারে এমন কম্পিউটার কোড লিখবেন না, কম্পাইল করবেন না, কপি করবেন না বা প্রচার করবেন না যা নিজে নিজেই প্রতিলিপি তৈরি করে, ক্ষতি করে বা যেকোন কম্পিউটার সিস্টেমের কার্যকারিতাকে বাধা দেয় (যেমন ভাইরাস, ওয়ার্ম, ট্রোজান, ইত্যাদি)।

x) যে কোনো ধরনের ভাইরাস অবিলম্বে রিপোর্ট করতে হবে।

xi) বিশেষজ্ঞের সহায়তা ছাড়া ভাইরাস পরিষ্কার/মোছা যাবে না যদি না অন্যথায় নির্দেশ দেওয়া হয়।

xii) ডেস্কটপ এবং ল্যাপটপ যখনই চালু বা পুনরায় চালু করা হবে তখন ব্যবহারকারী তার আইডি ও পাসওয়ার্ড ব্যবহার করে তা অ্যাক্সেস করতে হবে।

xiii) স্ট্যান্ডার্ড ভাইরাস শনাক্তকরণ সফ্টওয়্যার অবশ্যই সমস্ত ডেস্কটপ এবং ল্যাপটপ কম্পিউটারে ইনস্টল করতে হবে এবং এমনভাবে কনফিগার করতে হবে যাতে সিস্টেমটি পড়ার এবং নিয়মিতভাবে স্ক্যান করার সময় ভাইরাস শনাক্তের জন্য ফাইলগুলো পরীক্ষা করা হয়।

xiv) ডেস্কটপ এবং ল্যাপটপ কম্পিউটারগুলো সমস্ত গুরুত্বপূর্ণ কম্পিউটার নিরাপত্তা-প্রাসঙ্গিক ইভেন্ট (যেমন পাসওয়ার্ড অনুমান করা, অননুমোদিত অ্যাক্সেস প্রচেষ্টা, বা অ্যাপ্লিকেশন বা সিস্টেম সফ্টওয়্যার পরিবর্তন করা) লগ করার জন্য কনফিগার করতে হবে।

xv) সমস্ত কম্পিউটার ফ্লোর লেভেলের ওপরে এবং জানালা থেকে দূরে রাখতে হবে।

### ৫.৫.৩ বিওয়াইওডি নিয়ন্ত্রণ (BYOD Controls)

'Bring Your Own Device (BYOD)' হলো একটি অপেক্ষাকৃত নতুন অভ্যাস, যা ব্যাংক এবং আর্থিক প্রতিষ্ঠানগুলোর দ্বারা গৃহীত হয়—যাতে তাদের কর্মীদের তাদের ব্যক্তিগত মোবাইল ডিভাইস যেমন স্মার্টফোন, ট্যাবলেট কম্পিউটার ইত্যাদি থেকে কর্পোরেট ইমেইল, ক্যালেন্ডার, অ্যাপ্লিকেশন এবং ডেটা অ্যাক্সেস করতে সক্ষম করে। ব্যাংক বা এসবিএফআই কর্মীদের ব্যক্তিগত ডিভাইসগুলোকে সুরক্ষিত, পর্যবেক্ষণ এবং নিয়ন্ত্রণে চ্যালেঞ্জের কারণে বিওয়াইওডি-এর সঙ্গে সংশ্লিষ্ট উচ্চতর নিরাপত্তা ঝুঁকি সম্পর্কে সচেতন করতে হবে।

i) ব্যাংক বা এনবিএফআই বিওয়াইওডি বাস্তবায়নের ওপর একটি বিস্তৃত ঝুঁকি মূল্যায়ন করবে, যা নিশ্চিত করবে যে, বিওয়াইওডি-এর সঙ্গে সম্পর্কিত নিরাপত্তা ঝুঁকিগুলোকে প্রশমিত করার জন্য যথেষ্ট পরিমাণে ব্যবস্থা গ্রহণ করা হয়েছে।

ii) ব্যাংক বা এসবিএফআই যদি পর্যাপ্তভাবে সংশ্লিষ্ট নিরাপত্তা ঝুঁকিগুলো পরিচালনা করতে না পারে তাহলে বিওয়াইওডি বাস্তবায়ন করবে না।

iii) বিওয়াইওডি অনেক তথ্য নিরাপত্তা ঝুঁকির সঙ্গে যুক্ত যেমন—

ক) ব্যক্তিগত মালিকানাধীন ডিভাইসে (Personally Owned Devices বা POD) সংরক্ষিত কর্পোরেট ডেটার ক্ষতি, প্রকাশ বা দুর্নীতি।

খ) ব্যাংক বা এনবিএফআই এর আইসিটি অবকাঠামো এবং অন্যান্য তথ্য সম্পদের (যেমন ম্যালওয়্যার সংক্রমণ বা হ্যাকিং) হুমকি বা আপোস জড়িত ঘটনা,

গ) প্রযোজ্য আইন, প্রবিধান, এবং বাধ্যবাধকতাগুলোর সঙ্গে অসম্মতি (যেমন গোপনীয়তা বা পাইরেসি),

ঘ) ব্যাংক বা এনবিএফআই-এর জন্য কাজের সময় POD-এ তৈরি, সঞ্চিত, প্রক্রিয়া করা বা যোগাযোগ করা তথ্যের জন্য মেধা সম্পত্তি অধিকার (Intellectual Property rights)|

বিওয়াইওডি'র সঙ্গে সম্পর্কিত তথ্য নিরাপত্তা ঝুঁকির কারণে, বিওয়াইওডি-এ কাজ করতে ইচ্ছুক কর্মচারীদের অবশ্যই এটি করার জন্য অনুমোদন নিতে হবে এবং তাদের নিজস্ব সরঞ্জাম সুরক্ষিত করতে ব্যর্থ হওয়ার কারণে ব্যাংকের নেটওয়ার্কগুলোতে অগ্রহণযোগ্য ঝুঁকির কারণ হতে পারবে না।

iv) ব্যাংক বা এনবিএফআই কর্তৃপক্ষ দ্বারা অনুমোদিত পডগুলোর (POD) জন্য ডিভাইস অথেনটিকেশনের উপযুক্ত ফর্মগুলো প্রয়োগ করতে পারে, যেমন প্রতিটি নির্দিষ্ট ডিভাইসের জন্য তৈরি ডিজিটাল সার্টিফিকেট।

v) ব্যাংক বা এনবিএফআইর তথ্য নিয়ন্ত্রণ করার অধিকার রয়েছে। এর মধ্যে অবশ্যই পডস (PODs)-এর মালিক বা ব্যবহারকারীর অনুমতি ছাড়াই ব্যাকআপ, পুনরুদ্ধার, সংশোধন, অ্যাক্সেস নির্ধারণ এবং/অথবা ব্যাংক ডেটা মুছে ফেলার অধিকার অন্তর্ভুক্ত থাকতে হবে।

vi) সংবেদনশীল তথ্য অ্যাক্সেস, সঞ্চয় বা প্রক্রিয়া করতে ব্যবহৃত যেকোনো পডস (POD) অবশ্যই নেটওয়ার্কের মাধ্যমে স্থানান্তরিত ডেটা এনক্রিপ্ট করতে হবে (যেমন SSL বা VPN ব্যবহার করে)।

vii) ডিভাইসটি হারিয়ে গেলে, বা কর্মচারী চাকরি ছেড়ে দিলে, বা আইসিটি কোনো ডেটা বা নীতি লঙ্ঘন, ভাইরাস, বা ব্যাংকের ডেটা এবং প্রযুক্তি পরিকাঠামোর নিরাপত্তার জন্য অনুরূপ হুমকি শনাক্ত করলে, কর্মচারীর ডিভাইসটি মুছে ফেলতে হবে।

### ৫.৫.৪ সার্ভার নিরাপত্তা নিয়ন্ত্রণ (Server Security Controls)

i. ব্যবহারকারীদের জন্য নির্দিষ্ট সুযোগ সুবিধার বর্ণনাসহ সার্ভার অ্যাক্সেস করার জন্য নির্দিষ্ট অনুমোদন থাকতে হবে।

ii. দূরবর্তী ব্যবহারকারীদের (remote users) অ্যাক্সেস নিয়ন্ত্রণে অতিরিক্ত অথেনটিকেশন প্রক্রিয়া ব্যবহার করতে হবে।

iii. নিষ্ক্রিয়তার একটি নির্দিষ্ট সময়ের পরে নিষ্ক্রিয় সেশনের (Inactive session) মেয়াদ শেষ হবে।

iv. সিস্টেম অ্যাডমিনিস্ট্রেটর বা পদ্ধতি ব্যবস্থাপকদের কার্যকলাপ সীমিত করা হবে। সংবদনশীল ও গোপনীয় তথ্য ধারণকারী সার্ভারগুলোর কার্যকলাপ একটি কেন্দ্রীয় লগ হোস্টে সংরক্ষিত করতে পারে।

v. ব্যাংক বা এনবিএফআই উৎপাদন পদ্ধতিতে প্রয়োগের পূর্বে গঠনগত পদ্ধতি, নতুন Patches and service packs গুলো পরীক্ষা করার জন্য একটি প্ল্যাটফর্ম প্রস্তুত করতে এক বা একাধিক টেস্ট সার্ভার প্রস্তুত রাখবে।

vi. ব্যাংক বা এনবিএফআই ফাইল শেয়ারিং প্রক্রিয়ার নিরাপত্তা নিশ্চিত করবে। প্রয়োজন না হলে ফাইল ও প্রিন্ট শেয়ার অবশ্য নিষ্ক্রিয় করতে হবে বা যেখানে সম্ভব ন্যূনতম বজায় রাখা হবে।

vii. প্রোডাকশন সার্ভারে চলমান সমস্ত অপ্রয়োজনীয় পরিষেবাগুলো নিষ্ক্রিয় করা হবে। কোনো নতুন পরিষেবা যথাযথ পরীক্ষা ছাড়া উৎপাদন সার্ভারে স্থানান্তর করা যাবে না।

viii. সমস্ত অপ্রয়োজনীয় প্রোগ্রাম প্রোডাকশন সার্ভার থেকে আনইনস্টল করা হবে।

ix. ভার্চুয়ালাইজেশনের (virtualization) ক্ষেত্রে—

ক) ব্যাংক বা এনবিএফআই প্রতিটি VM দ্বারা সম্পদের (যেমন, প্রসেসর, মেমরি, ডিস্ক স্পেস, ভার্চুয়াল নেটওয়ার্ক ইন্টারফেস) ব্যবহারের সীমা নির্ধারণের পরিকল্পনা করবে।

খ) হোস্ট ও গেস্ট অপারেটিং সিস্টেম (OS) অবশ্য প্রয়োজনীয় নিরাপত্তা বিন্যাস এবং প্রয়োজনে অন্যান্য নিয়মের সঙ্গে হালনাগাদ করতে হবে। ভার্চুয়ালাইজেশন সফ্টওয়্যারে প্যাচিং (Patching) ব্যবহার করতে হবে।

গ) কাঠামোগত সার্ভারের মতো, ভার্চুয়াল সার্ভারগুলোকে নিয়মিত ব্যাক আপ করতে হবে।

ঙ) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে হোস্ট ও গেস্ট ওএস (OS) সমূহ সিঙক্রোনাইজেশন ব্যবহার করছে।

চ) প্রয়োজন না হলে হোস্ট ও গেস্ট ওএস-এর মধ্যে ফাইল শেয়ার করার অনুমতি দেওয়া হবে না।

### ৫.৫.৫. ডেটা সেন্টার নিয়ন্ত্রণ (Data Center Controls)

যেহেতু একটি ব্যাংক বা এনবিএফআই-এর ক্রিটিক্যাল সিস্টেম ও ডেটা একটি ডেটা সেন্টারে (ডিসি) সংরক্ষণ করা হয়, তাই এটি গুরুত্বপূর্ণ যে ডেটা সেন্টারটি স্থিতিস্থাপক (resilient) ও কাঠামোগতভাবে (physically) অভ্যন্তরীণ ও বাহ্যিকভাবে সুরক্ষিত।

#### ৫.৫.৫.১. কাঠামোগত নিরাপত্তা (Physical Security)

i. তথ্য প্রক্রিয়াকরণ এলাকা বা তথ্য কেন্দ্রে কাঠামোগত নিরাপত্তা কঠোরভবে প্রয়োগ করা হবে। ডিসিকে অবশ্যই কঠোর এলাকা ঘোষণা করতে হবে এবং তাতে অননুমোদিত প্রবেশ কঠোরভাবে নিষিদ্ধ করা হবে।

ii. ব্যাংক বা এবিএফআই শুধু অনুমোদিত কর্মীদের জন্য ডিসি-এর অ্যাক্সেস প্রদান করবে। ব্যাংক বা এনবিএফআই কেবল প্রয়োজনের ভিত্তিতে ডিসিতে অ্যাক্সেস দেবে। যদি এর আর প্রয়োজন না হয় তবে ডিসিতে কর্মীদের প্রবেশাধিকার অবিলম্বে প্রত্যাহার করা হবে।

iii. অ্যাক্সেস অনুমোদনের পদ্ধতিগুলো বিক্রেতা, পরিষেবা প্রদানকারী, সহায়তা কর্মী ও পরিচ্ছন্নতা কর্মীদের জন্য কঠোরভাবে প্রয়োগ করা হবে। ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে ডিসি-তে থাকাকালীন একজন ভিজিটরের সঙ্গে একজন কর্মচারী সর্বদা সঙ্গে থাকবেন।

iv. অ্যাক্সেস অনুমোদনের তালিকাটি রক্ষণাবেক্ষণ করা হবে এবং পর্যায়ক্রমে অনুমোদিত ব্যক্তি দ্বারা তথ্য কেন্দ্র অ্যাক্সেসের পর্যালোচনা করা হবে।

v. সংবেদনশীল এলাকায় অ্যাক্সেস করতে অবশ্যই অ্যাক্সেসের উদ্দেশ্য লগবুকে অন্তর্ভুক্ত করতে হবে।

vi. ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে ডিসির পরিধি, সুবিধা ও সরঞ্জাম কক্ষ কাঠামোগতভাবে (physically) সুরক্ষিত ও পর্যবেক্ষণ করা হয়েছে। ব্যাংক বা এনবিএফআই ২৪ ঘণ্টার জন্য মানব ও পদ্ধতিগত নিয়ন্ত্রণ প্রতিষ্ঠা করবে, যেমন নিরাপত্তারক্ষী, কার্ড অ্যাক্সেস পদ্ধতি, মানব সৃষ্ট ফাঁদ ও নজরদারি ব্যবস্থা, যেখানে যা উপযুক্ত।

vii. জরুরি প্রস্থান দরজা সহজলভ্য হবে।

viii. অনুমোদন প্রদান ও নীতির সঙ্গে সম্মতি নিশ্চিত করতে তথ্য কেন্দ্রে অবশ্য একজন মনোনীত অভিভাবক বা ব্যবস্থাপক থাকতে হবে।

ix. ব্যবস্থাপক বা প্রতিনিধিকে অবশ্য ডিসিতে থাকা সমস্ত কম্পিউটিং সরঞ্জাম, সংশ্লিষ্ট সরঞ্জাম ও ভোগ্য সামগ্রীর একটি তালিকা বজায় রাখতে হবে।

x. যেখানে একটি আউটসোর্সড পরিষেবা সরবরাহকারী ডিসি পরিচালনা করে, সেখানে ব্যাংক ও সরবরাহকারীর মধ্যে চুক্তিটি অবশ্যই নির্দেশ করবে যে, কাঠামোগত নিরাপত্তা সংক্রান্ত নীতির সমস্ত প্রয়োজনীয়তা তারা অবশ্য মেনে চলবে এবং ব্যাংক বা এনবিএফআই যে কোনো সময় কাঠামোগত নিরাপত্তা স্থিতি পর্যালোচনা করার অধিকার সংরক্ষণ করে।

xi. যেখানে ডিসি একটি আউটসোর্সড পরিষেবা সরবরাহকারী দ্বারা পরিচালিত হয়, সেখানে ভৌত নিরাপত্তার (physical security) দায়িত্ব সরবরাহকারীর ওপর বর্তায়, তবে এই ধরনের সুবিধাগুলোতে অ্যাক্সেস শুধু ব্যাংকের জন্য নিবেদিত, তা অবশ্যই ব্যাংক বা এনবিএফআই দ্বারা পর্যালোচিত ও অনুমোদিত হতে হবে।

xii. তথ্য কেন্দ্র প্রাঙ্গণের (Data Center Premises) ভৌত (physical) নিরাপত্তা প্রতি বছর অন্তত একবার পর্যালোচনা করা হবে।

#### ৫.৫.৫.২ পরিবেশগত নিরাপত্তা (Environmental Security)

i. আগুন, বন্যা, বিস্ফোরণ এবং অন্য ধরনের দুর্যোগের কারণে ক্ষতির ঝুঁকি থেকে তথ্য কেন্দ্রের সুরক্ষা পরিকল্পনা ও প্রয়োগ করা হবে। বহুবিধ (multi-tenant) সুবিধাযুক্ত ভবনে একটি তথ্য কেন্দ্র ও দুর্যোগ পুনরুদ্ধার সাইট তৈরি করা নিরুৎসাহিত করতে হবে।

ii. পাওয়ার সরবরাহ ও নেটওয়ার্ক সংযোগতাসহ তথ্য কেন্দ্রের ডিজাইন সঠিকভাবে নথিভুক্ত করা হবে।

iii. উন্নয়ন ও পরীক্ষার (Development and Test) পরিবেশ উৎপাদন প্রক্রিয়া থেকে পৃথক করা হবে।

iv. তথ্য কেন্দ্রে বাধা বা কোনো ধরনের ক্ষতি থেকে রক্ষা করতে তথ্য ও পাওয়ার ক্যাবলের জন্য পৃথক চ্যানেল তৈরি করতে হবে।

v. জল শনাক্তকরণ যন্ত্রগুলো উত্থাপিত (raised) মেঝের নিচে স্থাপন করা উচিত, যদি এটি উত্থাপিত হয়।

vi. তথ্য কেন্দ্রের সঙ্গে যুক্ত নয় এমন কোনও ডিভাইস এবং সব বন্ধ করা ডিভাইসগুলো তথ্য কেন্দ্রে সংরক্ষণ করার অনুমতি দেওয়া হবে না। সমস্ত

ধরনের অব্যবহৃত এবং অপ্রয়োজনীয় আইটি সরঞ্জাম (equipments) রাখতে একটি পৃথক সংরক্ষণাগার থাকতে হবে।

vii. ক্লোজড সার্কিট টেলিভিশন (সিসিটিভি) ক্যামেরা যথাযথ পর্যবেক্ষণের জন্য চারপাশে উপযুক্ত অবস্থানে স্থাপন করা হবে।

viii. 'খাওয়া, মদ্যপান বা ধূমপান নিষেধ' এর চিহ্ন প্রদর্শনে থাকবে।

ix. যেকোন জরুরি অবস্থার জন্য ডেডিকেটেড অফিসের যানবাহন সবসময় সাইটে উপস্থিত থাকবে। কোনো দুর্ঘটনার ঝুঁকি এড়াতে ব্যাংকের প্রাঙ্গণ বা কর্মাঙ্গনের বাইরে গুরুত্বপূর্ণ যন্ত্রপাতি বহন করার সময় গণপরিবহন এড়িয়ে চলতে হবে।

x. তথ্য কেন্দ্রে সার্বক্ষণিক টেলিফোন যোগাযোগ থাকবে।

xi. যেকোনো জরুরি প্রয়োজন মেটাতে সকল ব্যক্তির ঠিকানা এবং টেলিফোন বা মোবাইল নম্বর (যেমন ফায়ার সার্ভিস, পুলিশ স্টেশন, পরিষেবা প্রদানকারী, বিক্রেতা এবং সমস্ত আইসিটি কর্মী) অবশ্যই সহজলভ্য থাকতে হবে।

xii. পরিবেশগত হুমকি থেকে ঝুঁকি কমাতে বিদ্যুৎ সরবরাহ ব্যবস্থা এবং অন্যান্য সহায়তা ইউনিটকে অবশ্যই উৎপাদন স্থান (production site) থেকে আলাদা করতে হবে এবং নিরাপদ জায়গায় স্থাপন করতে হবে।

xiii. উৎস (প্রধান বিতরণ বোর্ড বা জেনারেটর) থেকে তথ্য কেন্দ্রে পাওয়ার সাপ্লাই অবশ্য নিবেদিত (dedicated) থাকতে হবে। ওভারলোডিংয়ের ঝুঁকি এড়াতে অন্য যেকোনো ডিভাইসের জন্য এই উৎসগুলো থেকে বৈদ্যুতিক সংযোগ নেওয়া যাবে না এবং এরুপ কাঠামোগুলোকে অবশ্য সীমাবদ্ধ (restricted) ও পর্যবেক্ষণ (monitored) করতে হবে।

xiv. নিম্নলিখিত পরিবেশগত নিয়ন্ত্রণগুলো ইনস্টল করতে হবে—

ক) ব্যাকআপ ইউনিটসহ নিরবচ্ছিন্ন পাওয়ার সরবরাহ (ইউপিএস)

খ) ব্যাকআপ পাওয়ার সরবরাহ।

গ) তাপমাত্রা এবং আর্দ্রতা পরিমাপের যন্ত্র।

ঘ) এয়ার কন্ডিশনার থেকে ওয়াটার লিকেজ সতর্কতা ও পানি নিষ্কাশন ব্যবস্থা।

ঙ) ব্যাকআপ ইউনিটসহ এয়ার কন্ডিশনার। প্রচলিত এয়ার কন্ডিশনার পদ্ধতি থেকে পানির ফুটো এড়াতে ইন্ডাস্ট্রি-স্ট্যান্ডার্ড এয়ার কন্ডিশনার পদ্ধতি ব্যবহার করতে হবে।

চ) জরুরি পাওয়ার কাট-অফ সুইচ।

ছ) জরুরি আলোর ব্যবস্থা।

জ) আর্দ্রতা নিয়ন্ত্রণের জন্য ডিহিউমিডিফায়ার

ঝ) উপরে উল্লিখিত পরিবেশগত নিয়ন্ত্রণগুলো নিয়মিত পরীক্ষা করা হবে এবং রক্ষণাবেক্ষণ পরিষেবা চুক্তি ২৪x৭ ভিত্তিক হবে।

### ৫.৫.৫.৩ আগুন প্রতিরোধ (Fire Prevention)

i) তথ্য কেন্দ্রের সিলিং ও দরজা আগুন-প্রতিরোধী হতে হবে।

ii) অগ্নি দমন সরঞ্জামগুলো পর্যায়ক্রমে ইনস্টল এবং পরীক্ষা করা হবে।

iii) স্বয়ংক্রিয় ফায়ার/স্মোক অ্যালার্মিং পদ্ধতি ইনস্টল করা এবং পর্যায়ক্রমে পরীক্ষা করতে হবে।

iv) উত্থাপিত ফ্লোরের নিচে ফায়ার ডিটেক্টর থাকতে হবে, যদি এটি উঁচু করা হয়।

v) তথ্য কেন্দ্রে বৈদ্যুতিক তার এবং ডেটা তারের গুণমান বজায় রাখতে হবে এবং লুকিয়ে রাখতে হবে।

vi) দাহ্য জিনিসপত্র যেমন কাগজ, কাঠের জিনিস, প্লাস্টিক ইত্যাদি তথ্য কেন্দ্রে সংরক্ষণ করার অনুমতি দেওয়া হবে না।

### ৫.৫.৬. সার্ভার/নেটওয়ার্ক রুম/র‍্যাক নিয়ন্ত্রণ (Server/Network Room/Rack Controls)

i) সার্ভার/নেটওয়ার্ক রুম/র‍্যাক অবশ্যই একজন দায়িত্বশীল ব্যক্তির অধীনে তালা ও চাবিসহ একটি কাচের ঘেরে থাকতে হবে।

ii) ফিজিক্যাল অ্যাক্সেস সীমাবদ্ধ থাকবে, দর্শনার্থী নিবন্ধন থাকতে হবে এবং সার্ভারের রুমে অ্যাক্সেসের ক্ষেত্রে তা লিপিবদ্ধ করতে হবে।

iii) অ্যাক্সেস অনুমোদনের তালিকাটি অবশ্য নিয়মিতভাবে বজায় রাখতে হবে এবং পর্যালোচনা করতে হবে।

iv) যেকোনো দুর্যোগের ক্ষেত্রে স্বল্পতম সময়ের মধ্যে সার্ভার ও নেটওয়ার্ক ডিভাইসগুলো প্রতিস্থাপনের ব্যবস্থা থাকবে।

v) সার্ভার/নেটওয়ার্ক রুম/র‍্যাক শীতাতপ নিয়ন্ত্রিত হতে হবে। জল ফুটো সংক্রান্ত সতর্কতা ও এয়ার কন্ডিশনার থেকে জল নিষ্কাশন ব্যবস্থা ইনস্টল করা হবে।

vi) বিদ্যুতের ব্যর্থতার ক্ষেত্রে কাজ চালিয়ে যাওয়ার জন্য পাওয়ার জেনারেটর থাকবে।

vii) সার্ভার ও প্রয়োজনীয় ডিভাইসগুলোতে নিরবচ্ছিন্ন বিদ্যুৎ সরবরাহের জন্য ইউপিএস থাকবে।

viii) অতিরিক্ত ডিভাইস সংযুক্ত করে যেন ইলেকট্রিক্যাল আউটলেটগুলোকে ওভারলোড না করা হয় সেই দিকে মনোযোগ দিতে হবে।

ix) পাওয়ার সরবরাহ ও ডাটা ক্যাবলের লে-আউট অনুসারে প্রাচীরের পাশের চ্যানেল প্রস্তুত করে সুগঠিত ও নিরাপদভাবে সমস্ত প্রয়োজনীয় ক্যাবলিং করতে হবে।

x) যেকোনও জরুরি পরিস্থিতি মোকাবেলার জন্য ফায়ার সার্ভিস, পুলিশ স্টেশন, পরিষেবা প্রদানকারী, বিক্রেতা এবং সমস্ত আইসিটি দায়িত্বশীল কর্মীদের সঙ্গে যোগাযোগের জন্য তাদের ঠিকানা এবং ফোন নম্বর সহজলভ্য থাকতে হবে।

xi) অন্যথায় প্রয়োজন না হলে, সার্ভার রুম ছেড়ে যাওয়ার আগে পাওয়ার সরবরাহ বন্ধ করে দিতে হবে।

xii) সার্ভার রুমের বাইরে দৃশ্যমান এলাকায় অগ্নি নির্বাপক যন্ত্র স্থাপন করা হবে। এটি বার্ষিক ভিত্তিতে পরীক্ষা করা আবশ্যক।

### ৫.৫.৭ নেটওয়ার্ক নিরাপত্তা ব্যবস্থাপনা (Network Security Management)

i) ব্যাংক বা এনবিএফআই অপারেটিং পদ্ধতি, ডেটাবেস, নেটওয়ার্ক সরঞ্জাম ও পোর্টেবল ডিভাইসগুলোর নিরাপত্তা নিশ্চিত করতে এমন বেসলাইন স্ট্যান্ডার্ড নির্নয় করবে যা সংস্থার নীতির সঙ্গে সামঞ্জস্যপূর্ন।

ii) বেসলাইন মানগুলো সমানভাবে প্রয়োগ করা হয়েছে এবং অসম্মতিগুলো শনাক্ত করা হয়েছে এবং তদন্তের জন্য উত্থাপন করা হয়েছে, তা নিশ্চিত করতে ব্যাংক বা এনবিএফআই নিয়মিত এনফোর্সমেন্ট চেক পরিচালনা করবে।

iii) নেটওয়ার্ক ডিজাইন এবং এর নিরাপত্তা কনফিগারেশনগুলো একটি নথিভুক্ত পরিকল্পনার অধীনে প্রয়োগ করা হবে। নেটওয়ার্ক ডিজাইনে সংজ্ঞায়িত বিভিন্ন নিরাপত্তা অঞ্চল নির্ধারিত থাকতে হবে।

iv) ইফটিপি, ফাইবার, এবং পাওয়ার ক্যাবলগুলো যাতে পরবর্তীতে সংশোধনমূলক বা প্রতিরোধমূলক রক্ষণাবেক্ষণের কাজ করা যায়, এর জন্য যথাযথ লেবেলিং থাকতে হবে।

v) ব্যাংক বা এনবিএফআই সমস্ত নেটওয়ার্ক সরঞ্জামের কাঠামোগত নিরাপত্তা নিশ্চিত করবে।

vi) তথ্য পরিষেবার গ্রুপ, ব্যবহারকারী ও তথ্য পদ্ধতিগুলোকে নেটওয়ার্কে আলাদা করা হবে, যেমন-ভিল্যান (VLAN)।

vii) অননুমোদিত ব্যবহার ও ইলেকট্রনিক টেম্পারিং কঠোরভাবে নিয়ন্ত্রণ করা হবে। একমুখী বা পাবলিক নেটওয়ার্কের মাধ্যমে ভ্রমণ করা সংবেদনশীল তথ্য এনক্রিপ্ট ও ডিক্রিপ্ট করার ব্যবস্থা থাকবে।

viii) আইসিটি অবকাঠামোর গুরুত্বপূর্ণ পর্যায়ে নেটওয়ার্ক সুরক্ষার উদ্দেশ্যে ব্যাংক বা এনবিএফআই নেটওয়ার্ক সুরক্ষা ডিভাইসগুলো ইনস্টল করবে, যেমন ফায়ারওয়াল এবং অনুপ্রবেশ শনাক্তকরণ ও প্রতিরোধ ব্যবস্থা (Intrusion Detection and Prevention Systems)।

ix) ব্যাংক বা এনবিএফআই অভ্যন্তরীণ নেটওয়ার্কগুলোর মধ্যে ফায়ারওয়াল বা অন্যান্য অনুরূপ ব্যবস্থা স্থাপন করবে, যাতে তৃতীয় পক্ষ, বিদেশি সিস্টেম এবং অভ্যন্তরীণ বিশ্বস্ত নেটওয়ার্ক থেকে উদ্ভূত নিরাপত্তা এক্সপোজারের প্রভাব কমিয়ে আনা যায়।

x) নিরাপদ লগইন বৈশিষ্ট্য (অর্থাৎ Secure Login Feature বা SSH) রিমোট অ্যাডমিনিস্ট্রেশনের উদ্দেশ্যে নেটওয়ার্ক ডিভাইসে সক্রিয় করা হবে। এনক্রিপ্টেড নয় এমন লগইন অপশন (যেমন, TELNET) নিষ্ক্রিয় করা হবে।

xi) ব্যাংক বা এনবিএফআই নিয়মিতভাবে নেটওয়ার্ক নিরাপত্তা ডিভাইসে নিয়মগুলো ব্যাক আপ করবে এবং পর্যালোচনা করবে যে এই ধরনের নিয়মগুলো উপযুক্ত ও প্রাসঙ্গিক কি না।

xii) ব্যাংক বা এনবিএফআই WAN সংযোগের জন্য রিডান্ডেন্ট যোগাযোগ ব্যবস্থা স্থাপন করবে।

xiii) ওয়্যারলেস লোকাল এরিয়া নেটওয়ার্ক (WLAN) স্থাপনকারী ব্যাংক বা এনবিএফআই এই পরিবেশের সঙ্গে সম্পর্কিত ঝুঁকি সম্পর্কে সচেতন থাকবেন। অ্যাক্সেস পয়েন্ট এবং ওয়্যারলেস ক্লায়েন্টদের মধ্যে যোগাযোগের জন্য সুরক্ষিত যোগাযোগ প্রোটোকলগুলো (Secure Communication Protocol) স্থাপন করতে হবে, যাতে অননুমোদিত অ্যাক্সেস থেকে কর্পোরেট নেটওয়ার্ককে সুরক্ষিত রাখা যায়।

xiv) নেটওয়ার্ক ডিভাইস দ্বারা তৈরি লগগুলো নিরীক্ষণের জন্য, নেটওয়ার্ক আকারের ওপর নির্ভর করে, SYSLOG-এ সার্ভার প্রতিষ্ঠা করা যেতে পারে।

xv) নেটওয়ার্ক ডিভাইসগুলো কার্যকরভাবে পরিচালনায়, নেটওয়ার্ক আকারের ওপর নির্ভর করে, প্রমাণীকরণ অনুমোদন ও অ্যাকাউন্টিং (Authentication, Authorization and Accounting-AAA) সার্ভার প্রতিষ্ঠা করা যেতে পারে।

xvi) নেটওয়ার্ক ট্রাফিক নিয়ন্ত্রণ করতে রাউটার (Router) গুলোতে রোলভিত্তিক এবং/অথবা সময়-ভিত্তিক অ্যাক্সেস কন্ট্রোল লিস্ট (ACLs) প্রয়োগ করতে হবে।

xvii) অবকাঠামো পরিচালনার জন্য সমস্ত নেটওয়ার্ক সরঞ্জাম এবং সার্ভারে একটি রিয়েল-টাইম হেল্‌থ পর্যবেক্ষণ পদ্ধতি প্রয়োগ করা যেতে পারে।

xviii) অফিস নেটওয়ার্কের সঙ্গে ব্যক্তিগত ল্যাপটপের সংযোগ বা অফিসের ল্যাপটপ/ডেস্কটপের সঙ্গে ব্যক্তিগত ওয়্যারলেস মডেমের সংযোগ অবশ্যই সীমাবদ্ধ ও সুরক্ষিত থাকতে হবে।

xix) ব্যাংক বা এনবিএফআই নেটওয়ার্ক ডিভাইসের সমস্ত ডিফল্ট (default) পাসওয়ার্ড পরিবর্তন করবে।

xx) অ্যাক্সেস সুইচের সমস্ত অব্যবহৃত পোর্ট ডিফল্টভাবে বন্ধ করা হবে যদি অন্যথায় সংজ্ঞায়িত না করা হয়।

xxi) সমস্ত যোগাযোগ ডিভাইস যথাযথ প্রমাণীকরণের (authentication) মাধ্যমে স্বতন্ত্রভাবে সনাক্তযোগ্য হতে হবে।

xxii) সার্ভারের জন্য রোল-ভিত্তিক প্রশাসন (role-based administration) নিশ্চিত করা হবে।

### ৫.৫.৮ ইন্টারনেট অ্যাক্সেস ম্যানেজমেন্ট (Internet Access Management)

i) অনুমোদিত ইন্টারনেট অ্যাক্সেস ব্যবস্থাপনা নীতি অনুসারে কর্মচারীদের ইন্টারনেট অ্যাক্সেস প্রদান করা হবে।

ii) ব্যাংক প্রাঙ্গন থেকে ইন্টারনেট অ্যাক্সেস ও ব্যবহার অবশ্য সুরক্ষিত হতে হবে এবং ব্যাংক বা এনবিএফআই-এর তথ্য নিরাপত্তার সঙ্গে আপস করা উচিত নয়।

iii) ব্যাংক প্রাঙ্গন থেকে ও ব্যাংকের সিস্টেমে ইন্টারনেট অ্যাক্সেস অবশ্যই নিরাপদ গেটওয়ের (Secure Gateway) মাধ্যমে চলাচল করতে হবে।

iv) ব্যাংক বা এনবিএফআই এর প্রাঙ্গণ বা সিস্টেম থেকে সরাসরি ইন্টারনেটের সঙ্গে যেকোনো সংযোগ, যার মধ্যে স্ট্যান্ড এলোন পিসি ও ল্যাপটপগুলো অন্তর্ভুক্ত, তথ্য সুরক্ষা দ্বারা অনুমোদিত না হওয়া পর্যন্ত নিষিদ্ধ।

v) কর্মচারীদের ব্যাংকের সিস্টেম বা প্রাঙ্গণ ব্যবহার করে ইন্টারনেটে তাদের নিজস্ব সংযোগ স্থাপন করা নিষেধ।

vi) ব্রডব্যান্ড, আইএসডিএন, বা পিএসটিএন পরিষেবার মাধ্যমে ইন্টারনেট বা কোনো তৃতীয়-পক্ষ বা পাবলিক নেটওয়ার্কের সঙ্গে সংযোগ স্থাপনের জন্য ব্যাংকের সিস্টেমগুলোর সঙ্গে স্থানীয়ভাবে সংযুক্ত মডেমের ব্যবহার সম্পূর্ন নিষিদ্ধ, যদি না নির্দিষ্টভাবে অনুমোদিত হয়।

vii) ব্যাংক বা এনবিএফআই দ্বারা প্রদত্ত ইন্টারনেট অ্যাক্সেস এমন কোনো বাণিজ্যিক ব্যবসায়িক কার্যকলাপ সম্পাদনের উদ্দেশ্যে করা যাবে না, যা ব্যাংক বা এনবিএফআই এর সঙ্গে সম্পর্কযুক্ত নয়। স্টাফ বা অন্যান্য কর্মিদের ব্যক্তিগত ব্যবসায়িক স্বার্থ ব্যাংকের ইন্টারনেট ব্যবহার করে পরিচালনা করা উচিত নয়।

viii) ব্যাংক বা এনবিএফআইও দ্বারা প্রদত্ত ইন্টারনেট অ্যাক্সেস অবশ্যই এমন কোনো কার্যকলাপে ব্যবহার করা উচিত নয়, যা জেনেশুনে কোনো ফৌজদারি বা দেওয়ানি আইন বা আইনের লঙ্ঘন করে। এই ধরনের যেকোনো কর্মকাণ্ডের ফলে জড়িত কর্মিদের শাস্তিমূলক ব্যবস্থা নেওয়া হবে।

ix) সমস্ত অ্যাপ্লিকেশন ও পদ্ধতি যেগুলোর জন্য ইন্টারনেট বা তৃতীয়-পক্ষ এবং পাবলিক নেটওয়ার্কগুলোর সঙ্গে সংযোগের প্রয়োজন হয়, তাদের অবশ্য ডেভেলপমেন্টের সময় এবং প্রোডাকশনে যাওয়ার আগে একটি আনুষ্ঠানিক ঝুঁকি বিশ্লেষণের মধ্য দিয়ে যেতে হবে এবং সমস্ত প্রয়োজনীয় নিরাপত্তা ব্যবস্থা অবশ্যই প্রয়োগ করতে হবে।

### ৫.৫.৯. ইমেইল ব্যবস্থাপনা (Email Management)

i) ইমেইল পদ্ধতি ব্যাংক বা এনবিএফআই-এর নীতিমালা অনুযায়ী ব্যবহার করা হবে।

ii) ইমেইল সিস্টেমে অ্যাক্সেস শুধু অফিসিয়াল অনুরোধের মাধ্যমে প্রদান করা হবে।

iii) অনুমোদিত এনক্রিপশন সুবিধাগুলো ব্যবহার করে এনক্রিপ্ট করা না হলে বহিরাগত দলগুলোর কাছে গোপনীয় তথ্য যোগাযোগ করতে ইমেইল ব্যবহার করা হবে না।

iv) ইমেইল পাঠানোর পূর্বে বা বহিরাগত দলগুলোকে উত্তর দেওয়ার পূর্বে কর্মচারিদের অবশ্যই সমস্ত ইমেল সামগ্রীর গোপনীয়তা ও সংবেদনশীলতা বিবেচনা করতে হবে।

v) ইমেইলের মাধ্যমে প্রেরিত তথ্য মানহানিকর, বা অপমানজনক হবে না, কোনো প্রকার জাতিগত বা যৌন নির্যাতনের সঙ্গে জড়িত, ব্যাংক বা এনবিএফআই-এর সুনাম নষ্ট করে, অথবা কর্মচারী, গ্রাহক, প্রতিযোগী বা অন্যদের জন্য ক্ষতিকর এমন কোনো উপাদান থাকতে পারে না। এই

ধরনের কোনো উপাদান ইচ্ছাকৃতভাবে প্রেরণের ফলে শাস্তিমূলক ব্যবস্থা নেওয়ার সম্ভাবনা রয়েছে।

vi) ব্যাংকের ইমেইল পদ্ধতিটি মূলত ব্যবসায়িক উদ্দেশ্যে ব্যবহারের জন্য প্রদান করা হয়। ব্যাংকের ইমেইল পদ্ধতির ব্যক্তিগত ব্যবহার শুধু ব্যবস্থাপনা কর্তৃপক্ষের বিবেচনায় অনুমোদন করা প্রয়োজন; এ ধরনের ব্যক্তিগত ব্যবহার যে কোনো সময় প্রত্যাহার বা সীমাবদ্ধ (restricted) হতে পারে।

vii) কর্পোরেট ইমেইল ঠিকানা অবশ্য কোনো সামাজিক নেটওয়ার্কিং, ব্লগ, গ্রুপ, ফোরাম, ইত্যাদির জন্য ব্যবহার করা যাবে না, যদি না ব্যবস্থাপনা কর্তৃপক্ষের অনুমোদন না থাকে।

viii) ব্যাংক বা এনবিএফআই থেকে ইমেল ট্রান্সমিশনের সঙ্গে একটি ডিসক্লেমার থাকতে হবে—যাতে ইমেলের বিষয়বস্তুর গোপনীয়তা রক্ষার বিষয় উল্লেখ থাকবে এবং নির্ধারিত প্রাপকের কাছে না পৌঁছালে তা মুছে ফেলতে অনুরোধ করা হবে।

ix) সংশ্লিষ্ট বিভাগ ইমেইল পরিষেবাগুলোর নিয়মিত পর্যালোচনা ও পর্যবেক্ষণ করবে।

### ৫.৬. ইনফরমেশন সিস্টেম ব্যবহার নিয়ন্ত্রণ (Access Control of Information System)

ব্যাংক বা এনবিএফআই শুধু কাজের দায়িত্বের ওপর ভিত্তি করে অ্যাক্সেসের অধিকার ও পদ্ধতি বিশেষাধিকার প্রদান করবে। ব্যাংক বা এনবিএফআই পরীক্ষা করবে যে রেঙ্ক বা পদের ভিত্তিতে কোনো ব্যক্তিরই বৈধ উদ্দেশ্যে গোপনীয় তথ্য, অ্যাপ্লিকেশন, পদ্ধতি সংস্থান বা সুবিধাগুলো অ্যাক্সেস করার কোনো অন্তর্নিহিত অধিকার নেই।

#### ৫.৬.১. ব্যবহারকারী অ্যাক্সেস ব্যবস্থাপনা (User Access Management)

i) ব্যাংক বা এনবিএফআই শুধু ব্যবহারকারীর প্রয়োজনের ভিত্তিতে আইসিটি সিস্টেম এবং নেটওয়ার্কগুলোতে একটি নির্ধারিত সময়ের জন্য অ্যাক্সেস মঞ্জুর করবে।

ii) ব্যাংক বা এনবিএফআই অ্যাক্সেস যেন না নিতে পারে, তার জন্য অ-কর্মচারীদের (চুক্তিভিত্তিক, আউটসোর্স বা ভেন্ডর কর্মীদের) নিবিড়ভাবে পর্যবেক্ষণ করবে।

iii) প্রতিটি ব্যবহারকারীর একটি অনন্য ব্যবহারকারী আইডি ও একটি বৈধ পাসওয়ার্ড থাকতে হবে।

iv) অ্যাক্সেসের সুবিধাসহ ব্যবহারকারী আইডি রক্ষণাবেক্ষণ ফর্ম যথাযথ কর্তৃপক্ষ দ্বারা অনুমোদিত হবে।

v) ব্যর্থ লগইন প্রচেষ্টার জন্য ব্যবহারকারীর অ্যাক্সেস বন্ধ করা হবে।

vi) কাজের দায়িত্ব পরিবর্তনের ক্ষেত্রে ব্যবহারকারীর অ্যাক্সেসের সুবিধাগুলো অবশ্যই হালনাগাদ রাখতে হবে।

vii) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে ব্যবহারকারীর অ্যাক্সেসের রেকর্ডগুলো স্বতন্ত্রভাবে চিহ্নিত করা হয়েছে এবং নিরীক্ষা ও পর্যালোচনার উদ্দেশ্যে লগ করা হয়েছে।

viii) ব্যাংক বা এনবিএফআই ব্যবহারকারীর অ্যাক্সেসের বিশেষাধিকারগুলোর (Privileges) নিয়মিত পর্যালোচনা করবে, যাতে নিশ্চিত করা যায় যে বিশেষাধিকারগুলো (Privileges) যথাযথভাবে দেওয়া হয়েছে।

#### ৫.৬.২. পাসওয়ার্ড ব্যবস্থাপনা (Password Management)

i) ব্যাংক বা এনবিএফআই ব্যবহারকারীদের অ্যাক্সেসের জন্য শক্তিশালী পাসওয়ার্ড ব্যবহার নিশ্চিত করবে।

ii) পাসওয়ার্ড নিয়ন্ত্রণে প্রথম লগইন করার সময় পাসওয়ার্ডের পরিবর্তন বাধ্যতামূলক থাকবে।

iii) পাসওয়ার্ড সংজ্ঞার প্যারামিটার এটা নিশ্চিত করবে যে, ব্যাংকের নীতি অনুযায়ী ন্যূনতম পাসওয়ার্ড দৈর্ঘ্য বজায় রাখা হয়েছে (অন্তত ৬ অক্ষর)।

iv) পাসওয়ার্ড হবে অন্তত তিন ধরনের অক্ষর যেমন বড় হাতের অক্ষর, ছোট হাতের অক্ষর, বিশেষ অক্ষর ও সংখ্যার সমন্বয়।

v) পাসওয়ার্ডের সর্বোচ্চ মেয়াদ ব্যাংকের নীতিমালায় অনুমোদিত দিনের সংখ্যার চেয়ে বেশি হবে না (সর্বোচ্চ ৯০ দিন)।

vi) ব্যাংকের নীতি অনুসারে (যেমন সর্বোচ্চ ৩ বার পরপর) ভুল লগইন প্রচেষ্টার সর্বাধিক সংখ্যা সঠিকভাবে নির্দিষ্ট করা হবে।

vii) পাসওয়ার্ড ইতিহাস রক্ষণাবেক্ষণ পদ্ধতিতে সক্রিয় করা হবে—যাতে একই পাসওয়ার্ড কমপক্ষে তিন (৩) বার পরে আবার ব্যবহার করা যায়।

viii) অপারেটিং সিস্টেম, ডাটাবেস ও ব্যবসায়িক অ্যাপ্লিকেশনগুলোর অ্যাডমিনিস্ট্রেটিভ পাসওয়ার্ডগুলো সিল করা খামে ভরে নিরাপদ হেফাজতে রাখা হবে।

**৫.৭. ব্যবসার ধারাবাহিকতা ও দুর্যোগ পুনরুদ্ধার ব্যবস্থাপনা (Business Continuity and Disaster Recovery Management)**

বিজনেস কন্টিনিটি ও ডিজাস্টার পুনরুদ্ধার ব্যবস্থাপনা হলো ক্রিটিক্যাল দুর্ঘটনা ও অপারেশনাল রিস্কের ক্ষেত্রে করনীয় ও প্রয়োজনীয় পরিকল্পনা তৈরি করা যাতে বিস্তৃত এলাকায় দুর্যোগ ব্যবস্থাপনা, ডেটা সেন্টার দুর্যোগ ব্যবস্থাপনা ও পুনরুদ্ধার পরিকল্পনা থাকে। বিজনেস কন্টিনিউটি প্ল্যানের (BCP) প্রাথমিক উদ্দেশ্য হলো একটি ব্যাংক বা NBFI-কে একটি দুর্যোগের মধ্যে টিকে থাকতে এবং নরমাল বিজনেস কার্যক্রম চালু করতে সক্ষম করা। ন্যূনতম আর্থিক ক্ষতি এবং সুনামের অবক্ষয় বজায় রাখতে, ব্যাংক বা NBFI-কে একটি যুক্তিসংগত সময়ের মধ্যে ক্রিটিক্যাল অপারেশনগুলো চালু করতে হবে। কন্টিনজেন্সি প্ল্যানের মধ্যে ব্যবসা পুনরুদ্ধারের পরিকল্পনা এবং দুর্যোগ পুনরুদ্ধার পরিকল্পনা অন্তর্ভুক্ত থাকবে। কন্টিনজেন্সি প্ল্যানিং-এ ব্যাকআপ, রিকোভারি ও রিস্টোর (restore) প্রক্রিয়াকেও অন্তর্ভুক্ত করবে।

**৫.৭.১. ব্যবসার ধারাবাহিকতা পরিকল্পনা (Business Continuity Plan-BCP)**

i) ব্যাংক বা এনবিএফআই-এর কাজকর্ম চালিয়ে যেতে দুর্যোগ থেকে পুনরুদ্ধারে একটি অনুমোদিত ব্যবসায়িক ধারাবাহিকতা পরিকল্পনা (BCP) থাকতে হবে।

ii) অনুমোদিত BCP সমস্ত প্রাসঙ্গিক অংশীদারদের কাছে প্রচার করা হবে। যখনই কোনো সংশোধন বা পরিবর্তন ঘটবে তখন অংশীদাররা সংশোধিত পরিকল্পনার একটি অনুলিপি পাবেন।

iii) বিসিপি সম্পর্কিত নথিগুলো অবশ্য একটি নিরাপদ দূরত্বে রাখতে হবে। তাৎক্ষণিক নির্দেশনার জন্য একটি অনুলিপি অফিসে সংরক্ষণ করা হবে।

iv) পদ্ধতি প্রয়োজনীয়তা, প্রক্রিয়া ও আন্তঃনির্ভরতার কথা বিবেচনা করে বিসিপি-কে ব্যবসায়িক প্রভাব বিশ্লেষণ (Business Impact Analysis-BIA) ও দুর্যোগ পুনরুদ্ধার পরিকল্পনা (Disaster Recovery Plan-DRP) দ্বারা সমন্বিত হতে হবে।

v) বিসিপি নিম্নলিখিত বিষয়গুলো নিশ্চিত করবে—

ক) নির্দিষ্ট সময়সীমার মধ্যে ব্যবসায়িক কার্যক্রম পুনরুদ্ধারের জন্য কর্ম পরিকল্পনা।

খ) কর্মকর্তা, ভেন্ডর ও বিভিন্ন সংস্থার জরুরি যোগাযোগ, ঠিকানা ও ফোন নম্বর।

গ) ব্যাকআপ টেপ, ল্যাপটপ, ফ্ল্যাশ ড্রাইভ, ইত্যাদি জরুরি আইটেমের গ্র্যাব লিস্ট (Grab List) তৈরি করা।

ঘ) দুর্যোগ পুনরুদ্ধারের সাইট ম্যাপ

ঙ) বিসিপি অবশ্যই বছরে অন্তত একবার পরীক্ষা ও পর্যালোচনা করতে হবে—যাতে এর কার্যকারিতা নিশ্চিত করা যায়।

**৫.৭.২. দুর্যোগ পুনরুদ্ধার পরিকল্পনা (Disaster Recovery Plan-DRP)**

i) ব্যাংক বা এনবিএফআই-এর একটি অনুমোদিত দুর্যোগ পুনরুদ্ধার পরিকল্পনা থাকতে হবে। একটি দ্রুত পুনরুদ্ধার পরিকল্পনা প্রণয়ন ও তৈরির ক্ষেত্রে, ব্যাংক বা এনবিএফআই বিভিন্ন ধরনের আকস্মিক পরিস্থিতি চিহ্নিত করবে এবং তা মোকাবেলায় Scenario Analysis অন্তর্ভুক্ত করবে। ব্যাংক বা এনবিএফআই এমন পরিস্থিতি বিবেচনা করবে যেমন—প্রধান সিস্টেমের বিভ্রাট যার ফলে সিস্টেম ত্রুটি, হার্ডওয়্যার ত্রুটি, পরিচালনার ত্রুটি, বা নিরাপত্তা সংক্রান্ত দুর্ঘটনা, এমনকি পাশাপাশি প্রাথমিক ডিসির সম্পূর্ণ অক্ষমতার কারণ হতে পারে।

ii) যখন প্রাথমিক সাইডে কোনো দুর্ঘটনা ঘটে, তখন ক্রিটিক্যাল সিস্টেমগুলো চালু করে ব্যবসা চালু করার উদ্দেশ্যে ব্যাংক বা এনবিএফআই একটি ডিজেস্টার রিকভারি সাইট (ডিআরএস) প্রতিষ্ঠা করবে যা ভৌগোলিকভাবে প্রাথমিক সাইট থেকে পৃথক (সর্বনিম্ন ১০ কিলোমিটার রেডিয়াল দূরত্ব তবে ভিন্ন ভূমিকম্প ঝুঁকিপূর্ণ অঞ্চলে)।

iii) যদি ডিজাস্টার রিকভারি সাইট (ডিআরএস) ভিন্ন সিসমিক জোনে না থাকে, তাহলে ব্যাংক বা এনএইচএফআই তৃতীয় ভিন্ন ভূমিকম্প অঞ্চলে একটি তৃতীয় সাইট স্থাপন করতে পারে যেটিকে ডিজাস্টার রিকভারি সাইট (ডিআরএস)/ ফার ডিসি হিসেবে ধরা হবে। এই ক্ষেত্রে, কাছাকাছি অবস্থানের DRS-কে নিয়ার ডিসি (Near DC) হিসাবে গণ্য করা হবে এবং সেই অনুযায়ী স্থাপন করতে হবে।

iv) ডিআরএস এবং/অথবা নিয়ার ডিসি বিপর্যয়ের ক্ষেত্রে ব্যবসা পরিচালনার গুরুত্বপূর্ণ পরিষেবাগুলোকে সমর্থন করতে সামঞ্জস্যপূর্ণ হার্ডওয়্যার ও টেলিযোগাযোগ সরঞ্জাম দিয়ে সজ্জিত করা উচিত।

v) ডিআরএস এবং/অথবা নিয়ার ডিসির কাঠামোগত ও পরিবেশগত নিরাপত্তা বজায় রাখা হবে।

vi) ব্যাংক বা এনবিএফআই সিস্টেম পুনরুদ্ধার এবং ব্যবসা পুনর্নির্মাণের অগ্রাধিকারগুলো সংজ্ঞায়িত করবে এবং আইসিটি পদ্ধতি ও অ্যাপ্লিকেশনগুলোর জন্য Recovery Time Objective (RTO) ও Recovery Point Objective (RPO) সহ নির্দিষ্ট পুনরুদ্ধারের প্রক্রিয়া স্থাপন করবে। আরটিও হলো ব্যাঘাতের বিন্দু থেকে সময়কাল—যার মধ্যে

একটি সিস্টেম পুনরুদ্ধার করা হবে। অন্যদিকে কোনো দুর্ঘটনা সংঘটিত হলে, আইসিটি সিস্টেমে কতটুকু ডেটা হারানো গ্রহণ করা যাবে, তা আরপিও দ্বারা বোঝায়।

vii) ব্যাংক বা এনবিএফআই তার পুনরুদ্ধার পরিকল্পনা করতে এবং তত্ত্বগত পরীক্ষা পরিচালনার ক্ষেত্রে গুরুত্বপূর্ণ পদ্ধতিগুলোর মধ্যে আন্তঃনির্ভরতা বিবেচনা করবে।

viii) ব্যাংক বা এনবিএফআই ব্যাংকের পুনরুদ্ধারের ক্ষমতা বাড়ানোর জন্য পুনরুদ্ধারের কৌশল ও প্রযুক্তি, যেমন- on-site redundancy Ges real time date replication অন্বেষণ করতে পারে।

ix) পুনরুদ্ধার প্রক্রিয়া জুড়ে তথ্য নিরাপত্তা সঠিকভাবে বজায় রাখা হবে।

x) ডিআর পরিকল্পনার হালনাগাদ ও পরীক্ষিত অনুলিপি নিরাপদ জায়গায় রাখা হবে। একটি অনুলিপি তাৎক্ষণিক নির্দেশনার জন্য অফিসে সংরক্ষণ করা হবে।

xi) ব্যাংক বা এনবিএফআই অন্তত বছরে একবার DRS-এর কার্যকারিতা এবং প্রয়োজনীয় জরুরি ও পুনরুদ্ধারের পদ্ধতিগুলো সম্পাদনায় কর্মীদের দক্ষতা পরীক্ষা ও যাচাই করবে।

xii) পুনরুদ্ধার করা পদ্ধতিগুলো সঠিকভাবে কাজ করছে কি না তা যাচাইয়ের জন্য ব্যাংক বা এনবিএফআই তার ব্যবহারকারীদের টেস্ট কেইস তৈরি ও সম্পাদনের ক্ষেত্রে সংশ্লিষ্ট করবে।

xiii) ডিআর পরীক্ষার নথিভুক্তকরণে ন্যূনতম Scope, পরিকল্পনা ও পরীক্ষার ফলাফল অন্তর্ভুক্ত থাকতে হবে। পরীক্ষার প্রতিবেদনগুলো ব্যবস্থাপনা এবং অন্যান্য স্টেকহোল্ডারের কাছে পাঠানো হবে এবং ভবিষ্যতে প্রয়োজনের জন্য সংরক্ষণ করা হবে।

### ৫.৭.৩ ডেটা ব্যাকআপ ও পুনরুদ্ধার ব্যবস্থাপনা (Data backup and Restore management)

i) ব্যাংক বা এনবিএফআই তথ্য ব্যাকআপ ও পুনরুদ্ধার নীতি তৈরি করবে। প্রতিটি ব্যবসায়িক অ্যাপ্লিকেশনের একটি পরিকল্পিত, নির্ধারিত ও নথিভুক্ত ব্যাকআপ কৌশল থাকতে হবে, যার মধ্যে অন এবং অফ-লাইন উভয় ব্যাকআপ তৈরি করা এবং অফসাইটে একটি সুরক্ষিত স্থানে ব্যাকআপ স্টোর করার নীতিমালা থাকবে।

ii) প্রতিটি ব্যবসায়িক অ্যাপ্লিকেশনের জন্য পরিকল্পিত ব্যাকআপ সূচি, অ্যাপ্লিকেশনের শ্রেণিবিভাগ এবং এটি সমর্থন করে এমন তথ্যের সঙ্গে সঙ্গতি রেখে তৈরি করতে হবে। এবং ব্যাকআপ সূচির প্রতিটি ক্ষেত্রে প্রয়োজনীয় ব্যাকআপের ধরন নির্দিষ্ট করতে হবে (সম্পূর্ণ, আংশিক, ইনক্রিম্যান্টাল, ডিফারেন্সিয়াল, রিয়েল-টাইম ইত্যাদি)।

iii) তথ্যের ব্যাকআপের ফ্রিকোয়েন্সি অবশ্যই তথ্যের শ্রেণিবিন্যাস এবং প্রতিটি অ্যাপ্লিকেশনের জন্য ব্যবসায়িক ধারাবাহিকতা পরিকল্পনার প্রয়োজনীয়তার সঙ্গে সঙ্গতিপূর্ণ হতে হবে।

iv) প্রতিটি ব্যবসায়িক অ্যাপ্লিকেশনের জন্য পরিকল্পিত ব্যাকআপ সূচির বিবরণে ব্যাক-আপ বা সংরক্ষণাগারভুক্ত তথ্যের জন্য রিটেনশন পিরিওড অন্তর্ভুক্ত থাকতে হবে, যা স্থানীয় আইনি ও নিয়ন্ত্রকের প্রয়োজনীয়তার সঙ্গে সামঞ্জস্যপূর্ণ হতে হবে।

v) ব্যাক-আপ তথ্য ধারণকারী সমস্ত মিডিয়ায় তথ্য বিষয়বস্তু, ব্যাকআপ চক্র, ব্যাকআপ ক্রম শনাক্তকারী, ব্যাকআপের তারিখ ও তথ্য সামগ্রীর শ্রেণিবিভাগ সংক্রান্ত লেবেল সংযুক্ত থাকতে হবে।

vi) ব্যাকআপ ইনভেন্টরি ও লগ শীট সুপারভাইজর কর্তৃক রক্ষণাবেক্ষণ ও পরীক্ষা করা ও স্বাক্ষর করা থাকতে হবে।

vii) ব্যাংক বা এনবিএফআই সংবেদনশীল বা গোপনীয় তথ্য স্টোরেজের জন্য অফ-সাইটে নেওয়ার পূর্বে টেপ বা ডিস্কে ব্যাকআপ তথ্য এনক্রিপ্ট করবে।

viii) ব্যাকআপের কমপক্ষে একটি অনুলিপি টাইম ক্রিটিক্যাল ডেলিভারির জন্য সাইটে রাখতে হবে।

ix) অন-এবং অফ-সাইট ব্যাকআপ থেকে তথ্য পুনরুদ্ধার করার প্রক্রিয়াটি অবশ্য নথিভুক্ত করা হবে।

x) ব্যাংক বা এনবিএফআই ব্যাকআপ মিডিয়ার পুনরুদ্ধার ক্ষমতার পর্যায়ক্রমিক পরীক্ষা ও পর্যবেক্ষণ চালাবে এবং মূল্যায়ন করবে যে এটি ব্যাংকের পুনরুদ্ধার প্রক্রিয়ার জন্য যথেষ্ট কার্যকর কি না।

## ৫.৮. তথ্য পদ্ধতি অধিগ্রহণ ও ডেভলাপমেন্ট (Acquisition and Development of Information Systems)

যে কোনো ব্যবসায়িক অ্যাপ্লিকেশন অধিগ্রহণ বা ডেভলাপমেন্টের পূর্বে, ব্যাংক বা NBFI কঠোর বিশ্লেষণ করে দেখে যে ব্যবসার প্রয়োজনীয়তাগুলো কার্যকর এবং দক্ষভাবে পূরণ করা হচ্ছে কি না। এ প্রক্রিয়াটিতে রয়েছে প্রয়োজনের সংজ্ঞা, বিকল্প উৎসের বিবেচনা, প্রযুক্তিগত ও অর্থনৈতিক সম্ভাব্যতার পর্যালোচনা, ঝুঁকি বিশ্লেষণ ও ব্যয়-সুবিধা বিশ্লেষণ এবং যার চূড়ান্ত সিদ্ধান্ত হবে তৈরি করা বা ক্রয় করা।

দুর্বল সিস্টেম পরিকল্পনা ও বাস্তবায়নের পাশাপাশি অপর্যাপ্ত পরীক্ষার কারণে অনেক সিস্টেম ব্যর্থ হয়। ব্যাংক বা এনবিএফআই পদ্ধতি পরিকল্পনা, উন্নয়ন ও যাচাইকরণ পর্যায়ে পদ্ধতি ঘাটতি ও ত্রুটি চিহ্নিত করবে। ব্যাংক বা এনবিএফআই একটি স্টেয়ারিং কমিটি গঠন করবে, যা ব্যবসার মালিক, প্রযুক্তিগত দল এবং অন্যান্য অংশীদারদের সমন্বয়ে প্রকল্পের অগ্রগতি ও মনিটরিং করবে। এর মাধ্যমে প্রকল্পের প্রতিটি পর্যায়কেই সহজলভ্য করা হবে এবং প্রকল্পের সময়সূচি অনুযায়ী মাইলফলকে পৌছা যাবে।

### ৫.৮.১ আইসিটি প্রকল্প ব্যবস্থাপনা (ICT Project Management)

i) একটি প্রজেক্ট ব্যবস্থাপনা রূপরেখা তৈরি করার সময়, ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে নতুন সিস্টেম তৈরি বা ক্রয়ের কাজ এবং প্রক্রিয়াগুলোর মধ্যে রয়েছে প্রকল্প ঝুঁকি মূল্যায়ন এবং শ্রেণিবিভাগ, প্রতিটি প্রকল্প পর্যায়ের জন্য গুরুত্বপূর্ণ সাফল্যের কারণ এবং প্রকল্পের মাইলফলক এবং ডেলিভারেবলের সংজ্ঞা। ব্যাংক বা এনবিএফআই প্রকল্প পরিচালনার কাঠামোতে, প্রকল্পের সঙ্গে জড়িত কর্মীদের ভূমিকা ও দায়িত্বগুলো স্পষ্টভাবে সংজ্ঞায়িত করবে।

ii) সমস্ত আইসিটি প্রকল্পের জন্য প্রকল্প পরিকল্পনা স্পষ্টভাবে নথিভুক্ত ও অনুমোদিত হবে। প্রকল্পের পরিকল্পনাগুলোতে, ব্যাংক বা এনবিএফআই প্রকল্পের প্রতিটি ধাপে বাস্তবায়িত করতে ডেলিভারেবল এবং সেইসঙ্গে নির্ধারিত মাইলফলকগুলো স্পষ্টভাবে নির্মাণ করবে।

iii) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে ব্যবহারকারীর ফাংশনাল প্রয়োজনীয়তা, খরচ-সুবিধা বিশ্লেষণ, পদ্ধতি প্রণয়ন, প্রযুক্তিগত বৈশিষ্ট্য, পরীক্ষার পরিকল্পনা ও পরিষেবা কর্মক্ষমতা প্রত্যাশা ইত্যাদি প্রাসঙ্গিক ব্যবসায়িক ইউনিট ও আইসিটি ব্যবস্থাপনা কর্তৃপক্ষ দ্বারা অনুমোদিত।

iv) ব্যাংক বা এনবিএফআই প্রকল্পের ব্যবস্থাপনার তত্ত্বাবধান স্থাপন করবে যাতে নিশ্চিত করা যায় যে মাইলফলকগুলো অর্জন করা সম্ভব হয়েছে এবং ডেলিভারেবলগুলো সময়মত বাস্তবায়িত হয়েছে।

### ৫.৮.২. সিস্টেম অধিগ্রহণের জন্য ভেন্ডর নির্বাচন (Vendor Selection for System Acquisition)

i) ভেন্ডর নির্বাচনের জন্য ফাংশনাল বিভাগ, আইসিটি বিভাগ ও ICC বিভাগের কর্মিদের সমন্বয়ে একটি কোর টিম থাকতে হবে।

ii) ভেন্ডর নির্বাচন প্রক্রিয়া অবশ্যই ব্যাংক বা এনবিএফআই-এর ক্রয় নীতির সঙ্গে সামঞ্জস্যপূর্ণ হতে হবে।

iii) অ্যাপ্লিকেশন ক্রয়ের জন্য ভেন্ডর নির্বাচনের ক্ষেত্রে নিম্নলিখিতগুলো বিবেচনা করতে হবে

ক) বাজারে উপস্থিতি (market presence)
খ) কার্যরত বছর (year in operation)
গ) প্রযুক্তি জোট (technology alliances)
ঘ) কাস্টমাইজেশনের পরিধি ও ওয়ার্ক এরাউন্ড সলিউশন
ঙ) আর্থিক শক্তি (financial strength)
চ) কর্মক্ষমতা ও বর্ধিত করার সুযোগ (performance and scalability)
ছ) ইনস্টলেশনের সংখ্যা
জ) বিদ্যমান গ্রাহকের রেফারেন্স
ঝ) সমর্থন ব্যবস্থা (support arrangement)
ঞ) বিদেশি বিক্রেতাদের জন্য স্থানীয় সহায়তা ব্যবস্থা
ট) আর্থিক ও প্রযুক্তিগত প্রস্তাবের গুরুত্ব

### ৫.৮.৩. ইন-হাউস সফ্টওয়্যার ডেভলাপমেন্ট (In-House Software Developement)

i) বিশদ ব্যবসায়ের প্রয়োজনীয়তাগুলো নথিভুক্ত ও উপযুক্ত কর্তৃপক্ষ দ্বারা অনুমোদিত হবে।

ii) বিস্তারিত প্রযুক্তিগত প্রয়োজনীয়তা ও নকশা প্রস্তুত করা হবে।

iii) অ্যাপ্লিকেশন নিরাপত্তা এবং প্রাপ্যতার প্রয়োজনীয়তা সুরাহা করা হবে।

iv) অ্যাপ্লিকেশনে তৈরিকৃত কার্যকারিতা, পরিকল্পনা ও নথিভুক্তকরণ অনুযায়ী হতে হবে।

v) সফটওয়্যার তৈরি ও বাস্তবায়নের পর্যায়ে User Acceptance Test (UAT) mn Software Development Life Cycle (SDLC) পরিচালনা করতে হবে।

vi) সফটওয়্যার তৈরি হওয়ার পরে User Verification Test (UVT) করতে হবে।

vii) সিস্টেম ডকুমেন্ট ও ইউজার ম্যানুয়াল তৈরি করা হবে এবং সংশ্লিষ্ট বিভাগের কাছে হস্তান্তর করা হবে।

viii) সোর্স কোড (Source Code) অবশ্যই সংশ্লিষ্ট বিভাগের কাছে হস্তান্তর করতে হবে এবং তা সুরক্ষিত রাখতে হবে।

ix) সোর্স কোডে লেখকের নাম, সৃষ্টির তারিখ, পরিবর্তনের শেষ তারিখ এবং অন্যান্য প্রাসঙ্গিক তথ্যসহ একটি শিরোনাম থাকতে হবে।

x) অ্যাপ্লিকেশনটি ব্যাংকের আইসিটি নিরাপত্তা নীতির সঙ্গে সঙ্গতিপূর্ণ হতে হবে।

xi) ব্যাংক বা এননবিএফআই অবশ্যই নিয়ন্ত্রকের কমপ্লায়েন্সের দিকে দৃষ্টি রাখবে।

## ৫.৯. অল্টারনেটিভ ডেলিভারি চ্যানেল (এডিসি) নিরাপত্তা ব্যবস্থাপনা (Alternative Delivery Channel Security Management)

'চ্যানেলের মাধ্যমে চ্যানেল' হলো আজকের ব্যাংকিংয়ের নতুন উদ্ভাবন, যা আগে শুধু শাখা নেটওয়ার্কের ওপর নির্ভর করত। শাখাবিহীন ব্যাংকিং হলো একটি ডিস্ট্রিবিউশন চ্যানেল কৌশল, যা ব্যাংকের শাখার ওপর নির্ভর না করে আর্থিক পরিষেবা প্রদান করে থাকে। বিকল্প ডেলিভারি চ্যানেল হলো গ্রাহকদের সরাসরি ব্যাংকিং পরিষেবা প্রদানের একটি বিকল্প পদ্ধতি। গ্রাহকরা তাদের এটিএম-এর মাধ্যমে ব্যাংকিং লেনদেন করতে পারেন, যেকোনো অনুসন্ধানের জন্য ব্যাংকের কল সেন্টারে যোগাযোগ করতে পারেন, ডিজিটাল ইন্টারঅ্যাকটিভ ভয়েস রেসপন্স (আইভিআর) অ্যাক্সেস করতে পারেন, ইন্টারনেট ব্যাংকিংয়ের মাধ্যমে এমনকি মোবাইল ব্যাংকিংয়ের মাধ্যমে ফোনেও লেনদেন করতে পারেন ইত্যাদি। ঐ চ্যানেলসমূহ সময় ও ভৌগোলিক অবস্থান নির্বিশেষে একটি বিস্তৃত গ্রাহকগোষ্ঠীকে ব্যাংকিং সার্ভিস প্রদান করে। এডিসি কম অপারেশনাল ব্যয়ে ও কম লেনদেন খরচে উচ্চতর গ্রাহক সন্তুষ্টি নিশ্চিত করে।

### ৫.৯.১. এটিএম/পিওএস লেনদেন (ATM/POS Transaction)

এটিএম এবং পয়েন্ট-অফ-সেল (পিওএস) ডিভাইসগুলো কার্ড ব্যবহারকারীদের নগদ অর্থ তোলার পাশাপাশি ব্যবসায়ী এবং বিলিং সংস্থাগুলোর বিল পেমেন্ট সুবিধা দিয়েছে। কিন্তু এই পদ্ধতিগুলো প্রায়ই কার্ড স্কিমারদের (skimmers) লক্ষ্যবস্তুতে পরিনত হয়।

এই পদ্ধতিগুলো ব্যবহার করার ক্ষেত্রে গ্রাহকদের আস্থা সুরক্ষিত করার জন্য, ব্যাংক বা এনবিএফআই, প্রতারকদের আক্রমণ প্রতিহত করার জন্য এটিএম এবং POS ডিভাইসগুলোতে নিম্নলিখিত ব্যবস্থাগুলো স্থাপন করবে—

i) ব্যাংক বা এনবিএফআই একটি কার্ড এন্ট্রি স্লটের ওপরে বা কাছাকাছি অজানা ডিভাইসগুলোর উপস্থিতি (presence of unknown devices) শনাক্ত করতে এটিএম ডিভাইসগুলোতে অ্যান্টি-স্কিমিং ডিভাইস (anti-skimming device) ইনস্টল করবে।

ii) ব্যাংক বা এনবিএফআই শনাক্তকরণ ব্যবস্থা ইনস্টল করবে এবং ফলো-আপ প্রতিক্রিয়া (response) ও পদক্ষেপের (action) জন্য উপযুক্ত কর্মীদের সতর্কতা বার্তা পাঠাবে।

iii) ট্রান্সমিশনের সময় গ্রাহকদের পিন এনক্রিপ্ট করা হয়েছে তা নিশ্চিত করতে ব্যাংক বা এনবিএফআই টেম্পার-প্রতিরোধী (temper-resistant) কীপ্যাড ব্যবহার করবে।

iv) ব্যাংক বা এনবিএফআই শোল্ডার সার্ফিংয়ের (shoulder surfing) মাধ্যমে গ্রাহকদের পিন জেনে ফেলা প্রতিরোধের উপযুক্ত ব্যবস্থা করবে।

v) ব্যাংক বা এনবিএফআই পিন আপস (Compromise) প্রতিরোধ করার জন্য বায়োমেট্রিক ফিঙ্গার ভেইন সেন্সিং প্রযুক্তি (Biometric Finger Vein Security Technology) প্রয়োগ করতে পারে।

vi) ব্যাংক বা এনবিএফআই এই মেশিনগুলোতে ২৪ ঘন্টা কার্যকলাপের ভিডিও নজরদারি পরিচালনা করবে, সিসিটিভি ফুটেজের গুণমান বজায় রাখবে এবং এটি কমপক্ষে এক বছরের জন্য সংরক্ষণ করবে।

vii) ব্যাংক বা এনবিএফআই নগদ ব্যালেন্স, লোডিং-আনলোডিং কার্যাবলি, মেশিনের অকার্যকারিতা ইত্যাদির জন্য একটি কেন্দ্রীভূত অনলাইন মনিটরিং পদ্ধতি চালু করবে।

viii) ব্যাংক বা এনবিএফআই ২৪-ঘণ্টা ভিত্তিতে সমস্ত এটিএম ডিভাইসের জন্য নিরাপত্তা কর্মী মোতায়েন করবে।

ix) ব্যাংক বা এনবিএফআই যাচাই করবে যে এটিএম ডিভাইসগুলোতে পর্যাপ্ত কাঠামোগত নিরাপত্তা ব্যবস্থা প্রয়োগ করা হয়েছে।

x) ব্যাংক বা এনবিএফআই সমস্ত এটিএম/পিওএস ডিভাইসগুলোকে ঘন ঘন পরিদর্শন করবে যাতে স্ট্যান্ডার্ড প্র্যাকটিস (যেমন, এটিএম-এর জন্য পরিবেশগত নিরাপত্তা, এটিএম-এর জন্য অ্যান্টি-স্কিমিং ডিভাইস, পিওএস ডিভাইসের সারফেস টেম্পারিং, ইত্যাদি) প্রয়োজনীয় কমপ্লায়েন্স সহ বজায় থাকে। পরিদর্শন লগ শীট এটিএম বুথ প্রাঙ্গনে ও কেন্দ্রীয়ভাবে রক্ষণাবেক্ষণ করা হবে।

xi) ব্যাংক বা এনবিএফআই নিয়মিতভাবে তৃতীয় পক্ষের নগদ পুনঃপূরণ (cash replenishment) ভেন্ডরদের কার্যক্রম নিরীক্ষণ করবে এবং নিয়মিতভাবে তৃতীয় পক্ষের ক্যাশ সর্টিং হাউজ (cash sorting house) পরিদর্শন করবে।

xii) ব্যাংক বা এনবিএফআই তার মার্চেন্টদেরকে পিওএস ডিভাইস পরিচালনা করার প্রয়োজনীয় (যেমন স্বাক্ষর যাচাইকরণ, ডিভাইস

টেম্পারিং/প্রতিস্থাপনের প্রচেষ্টা, ডিফল্ট পাসওয়ার্ড পরিবর্তন ইত্যাদি সম্পর্কে) প্রশিক্ষণ দিবে এবং প্রয়োজনীয় ম্যানুয়াল প্রদান করবে।

১. ব্যাংক বা এনবিএফআই যে সমস্ত নিরাপত্তা ব্যবস্থা গ্রহণ করেছে এবং এটিএম ও পিওএস লেনদেনের সময় গ্রাহকদের দ্বারা অনুসরণ করতে হবে, তা সম্বন্ধে গ্রাহকদের শিক্ষিত করবে।

### ৫.৯.২ ইন্টারনেট ব্যাংকিং (Internet Banking)

পাবলিক নেটওয়ার্কের মধ্য দিয়ে যাওয়া ইন্টারনেট ব্যাংকিং সুবিধার সঙ্গে সম্পৃক্ত তথ্য সমূহ প্রতারণামূলক কার্যকলাপ, বিরোধ (dispute) ও অননুমোদিত প্রকাশ বা পরিবর্তন থেকে সুরক্ষিত রাখতে হবে। ইন্টারনেটের মাধ্যমে প্রদানকৃত আর্থিক পরিষেবাগুলো ক্রমবর্ধমানভাবে বৃদ্ধি পাওয়ার কারণে ব্যাংকগুলোর ইন্টারনেট পদ্ধতি যথেষ্ট Vulnerable হতে পারে। এটির সুরক্ষা হিসাবে, ব্যাংক বা এনবিএফআই একটি নিরাপত্তা কৌশল প্রণয়ন করবে এবং তার তথ্য এবং পদ্ধতিগুলোর গোপনীয়তা, অখণ্ডতা ও প্রাপ্যতা নিশ্চিত করতে ব্যবস্থা গ্রহণ করবে।

i) ব্যাংক বা এনবিএফআই তার গ্রাহকদের এবং ব্যবহারকারীদের নিশ্চয়তা প্রদান করবে যাতে ইন্টারনেটের মাধ্যমে সম্পাদিত অনলাইন অ্যাক্সেস ও লেনদেনগুলো পর্যাপ্তভাবে সুরক্ষিত ও অথেনটিকেটেড হয়।

ii) ব্যাংক বা এনবিএফআই তার ইন্টারনেট ব্যাংকিং পদ্ধতি সঙ্গে সম্পর্কিত নিরাপত্তার প্রয়োজনীয়তাগুলোকে যথাযথভাবে মূল্যায়ন করবে এবং আন্তর্জাতিক মানে সুপ্রতিষ্ঠিত করার ব্যবস্থা গ্রহণ করবে।

iii) ব্যাংক বা এনবিএফআই প্রযুক্তিগত নিরাপত্তার দিকগুলো এবং অপারেশনাল ইস্যুগুলো বিবেচনা করে একটি ইন্টারনেট ব্যাংকিং নিরাপত্তা নীতিমালা প্রণয়ন করবে।

iv) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে ব্যাংক এবং এর গ্রাহকদের মধ্যে প্রক্রিয়া করা, সংরক্ষিত বা প্রেরণ করা তথ্য সঠিক, নির্ভরযোগ্য এবং সম্পূর্ণ। ব্যাংক বা এনবিএফআই পদ্ধতি এবং ডেটার অখণ্ডতা রক্ষা করার জন্য উপযুক্ত প্রক্রিয়াকরণ এবং সংক্রমণ নিয়ন্ত্রণও প্রয়োগ করবে, যেমন SSL, TLS।

v) সব ধরনের অনলাইন আর্থিক লেনদেনের জন্য ব্যাংক 2FA (দ্বি-ফ্যাক্টর প্রমাণীকরণ) প্রয়োগ করবে। হার্ডওয়্যার/সফ্টওয়্যার-ভিত্তিক টোকেনাইজেশন পদ্ধতি প্রাধান্য দেয়া হবে। দ্বি-ফ্যাক্টর প্রমাণীকরণের প্রাথমিক উদ্দেশ্যগুলো হলো গ্রাহকের প্রমাণীকরণ প্রক্রিয়াকে সুরক্ষিত করা এবং গ্রাহকের অ্যাকাউন্টের তথ্য ও লেনদেনের বিবরণের অখণ্ডতা রক্ষা করা এবং সেইসঙ্গে অনলাইন পদ্ধতিতে আস্থা বাড়ানো।

vi) একটি অনলাইন কার্যক্রম একটি নির্দিষ্ট সময়ের পরে স্বয়ংক্রিয়ভাবে সমাপ্ত হতে হবে যদি না গ্রাহক বিদ্যমান সেশনটি বজায় রাখার জন্য পুনরায় অথেনটিকেট করেন।

vii) ব্যাংক বা এনবিএফআই পরবর্তীতে সিস্টেমের অস্বাভাবিক কার্যকলাপ, ট্রান্সমিশন ত্রুটি, বা অস্বাভাবিক অনলাইন লেনদেনগুলো অনুসরণ ও মোকাবেলার জন্য পর্যাপ্ত পর্যবেক্ষণ বা নজরদারি ব্যবস্থা গ্রহন করবে।

viii) প্রাপ্ত বার্তাসহ সিস্টেমে প্রবেশের সফল লগ রেকর্ড করা হবে। নিরাপত্তা লঙ্ঘন (সন্দেহ বা চেষ্টা) রিপোর্ট করা হবে এবং নজরদারি করা হবে। ব্যাংক অনুপ্রবেশ ও আক্রমণ প্রতিরোধের জন্য সিস্টেম ও নেটওয়ার্ক পর্যবেক্ষণ সরঞ্জাম স্থাপন করতে পারে।

ix) ব্যাংক বা এনবিএফআই অনলাইন পদ্ধতি ও সাপোর্টিং পদ্ধতিগুলো (যেমন ইন্টারফেস সিস্টেম, ব্যাকএন্ড হোস্ট সিস্টেম ও নেটওয়ার্ক সরঞ্জাম) এর উচ্চ স্থিতিস্থাপকতা (resilience) ও প্রাপ্যতা (availability) বজায় রাখবে। ব্যাংক বা এনবিএফআই সক্ষমতা ব্যবহারের পরিকল্পনা করার পাশাপাশি অনলাইন আক্রমণ থেকে রক্ষায় ব্যবস্থা গ্রহণ করবে। এই অনলাইন আক্রমণগুলোর মধ্যে Denial of Service (DOS) আক্রমন ও Distributed Denial of Service (DDOS) আক্রমণ অন্তর্ভুক্ত থাকতে পারে।

x) ব্যাংক বা এনবিএফআই অন্যান্য ধরনের আক্রমণ কমানোর জন্য যথাযথ ব্যবস্থা গ্রহণ করবে যেমন Middleman আক্রমণ, যা সাধারণত ম্যান-ইন-দ্য-মিডল অ্যাটাক (MITMA), ম্যান-ইন-দ্য-ব্রাউজার আক্রমণ, অথবা ম্যান-ইন-দ্য অ্যাপ্লিকেশান আক্রমণ হিসাবে পরিচিত।

xi) তথ্য নিরাপত্তা অফিসার বা অন্য যেকোন অর্পিত ব্যক্তি/টিম সিস্টেমের পর্যায়ক্রমিক Penetration Test গ্রহণ করবে, যার মধ্যে অন্তর্ভুক্ত থাকতে পারে:

ক) পাসওয়ার্ড ট্র্যাকিং টুল ব্যবহার করে পাসওয়ার্ড অনুমান করার চেষ্টা করা।

খ) কম্পিউটার প্রোগ্রামে Back Door Traps খোঁজা।

গ) ডিডিওএস (Distributed Denial of Service) ও ডিওএস (Denial of Service) আক্রমণ ব্যবহার করে সিস্টেমটিকে ওভারলোড করার চেষ্টা করা।

ঘ) Middleman আক্রমণ চেক করা।

ঙ) সফ্টওয়্যার, বিশেষ করে ব্রাউজার ও ই-মেইল সফ্টওয়্যারের মধ্যে সাধারণভাবে পরিচিত Holes পরীক্ষা করা

চ) অবকাঠামোর দুর্বলতা পরীক্ষা করা

ছ) পোর্টের নিয়ন্ত্রণ নেওয়া
জ) অ্যাপ্লিকেশন Crash হওয়ার কারণ বের করা
ঝ) অ্যাপ্লিকেশন ও ডাটাবেস সার্ভারে দূষিত কোডগুলো ইনজেক্ট করা
ঞ) ব্যাংক বা এনবিএফআই তার গ্রাহকদের একটি অনলাইন পরিবেশে কীভাবে সুরক্ষা পাওয়া যায় তা সম্পর্কে শিক্ষিত করবে।

### ৫.৯.৩ পেমেন্ট কার্ড (Payment Cards)

পেমেন্ট কার্ড, কার্ডধারীদের যে কোনো জায়গায় কেনাকাটা করতে শিথিলতা দেয়। কেনাকাটার পর বিল পেমেন্টের জন্য কার্ডধারীরা মার্চেন্টের কাছে অর্থপ্রদানের জন্য এই কার্ডগুলো বস্তুগতভাবে (physically) উপস্থাপন করে বা কার্ড ব্যবহার করে তারা ইন্টারনেটে, মেইল-অর্ডারের মাধ্যমে বা টেলিফোনের মাধ্যমে কেনাকাটার বিল পরিশোধ করতে পারে। পেমেন্ট কার্ডগুলো কার্ডধারকদের অটোমেটেড টেলার মেশিনে ('এটিএম') নগদ অর্থ তোলার সুবিধাও দেয়।

পেমেন্ট কার্ড অনেক আকারে বিদ্যমান; ম্যাগনেটিক স্ট্রাইপ কার্ডের সঙ্গে সর্বোচ্চ নিরাপত্তা ঝুঁকি হয়। ম্যাগনেটিক স্ট্রাইপ কার্ডে সংরক্ষিত সংবেদনশীল পেমেন্ট কার্ড তথ্য কার্ড স্কিমিং (card skimming) আক্রমণের জন্য ঝুঁকিপূর্ণ। এটিএম, পেমেন্ট কিয়স্ক (kiosk) এবং পিওএস টার্মিনালসহ পেমেন্ট কার্ড প্রক্রিয়াকরণের বিভিন্ন পয়েন্টে কার্ড স্কিমিং আক্রমণ ঘটতে পারে।

i) পেমেন্ট কার্ড পরিষেবা প্রদানকারী ব্যাংক বা এনবিএফআই সংবেদনশীল পেমেন্ট কার্ড তথ্য সুরক্ষিত করতে পর্যাপ্ত সুরক্ষা ব্যবস্থা বাস্তবায়ন করবে। ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে সংবেদনশীল কার্ড-এর তথ্য এনক্রিপ্ট করা হয়েছে যাতে স্টোরেজ ও ট্রান্সমিশনে এই তথ্যগুলোর গোপনীয়তা ও অখণ্ডতা নিশ্চিত করা যায়।

ii) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে সংবেদনশীল বা গোপনীয় তথ্যের প্রক্রিয়াকরণ একটি নিরাপদ পরিবেশে করা হয়েছে।

iii) ব্যাংক বা এনবিএফআই সংবেদনশীল পেমেন্ট কার্ডে তথ্য সংরক্ষণ করতে একাধিক পেমেন্ট অ্যাপ্লিকেশন সমর্থিত সুরক্ষিত চিপ স্থাপন করবে। Interoperability এর কারণে, যেখানে শুধু কার্ডের ম্যাগনেটিক স্ট্রাইপ থেকে তথ্য পড়তে হয়, সেখানে ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে এই লেনদেনগুলো পরিচালনা করতে পর্যাপ্ত নিয়ন্ত্রণ প্রয়োগ করা হয়েছে।

iv) ব্যাংক বা এনবিএফআই গ্রাহকদের সংবেদনশীল স্ট্যাটিক তথ্য যেমন পিন বা পাসওয়ার্ডের অথেনটিকেশন সম্পাদন করবে। ব্যাংক বা এনবিএফআই তার Service Providers দ্বারা ব্যবহৃত অবকাঠামো ও প্রক্রিয়াগুলোর নিয়মিত নিরাপত্তা পর্যালোচনা করবে।

v) পেমেন্ট কার্ডের পিন এবং কীগুলো (keys) তৈরি করতে ব্যবহৃত সরঞ্জামগুলো নিরাপদ পদ্ধতিতে পরিচালনা করা হবে।

vi) কার্ড ব্যক্তিগতকরণ (card personalisation), পিন তৈরি, কার্ড বিতরণ, পিন বিতরণ ও কার্ড সক্রিয়করণ (activation) পদ্ধতি প্রতিটি একে অপরের থেকে আলাদা হতে হবে।

vii) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে নিরাপত্তা নিয়ন্ত্রণগুলো পেমেন্ট কার্ড সিস্টেম ও নেটওয়্যার্কে প্রয়োগ করা হয়েছে এবং ব্যাংক বা এনবিএওফআই অবশ্যই কার্ডধারীর তথ্যর নিরাপত্তা নিশ্চিত করতে Industry Security Standard মেনে চলবে, যেমন পেমেন্ট কার্ড ইন্ডাস্ট্রি সিকিউরিটি স্ট্যান্ডার্ড (PCI-DSS)।

viii) ব্যাংক বা এনবিএফআই শুধু গ্রাহকের অনুরোধ পাওয়ার পর নতুন পেমেন্ট কার্ড সক্রিয় করবে।

ix) ব্যাংক বা এনবিএফআই ইন্টারনেটের মাধ্যমে কার্ড নট-প্রেজেন্ট (CNP) ধরনের লেনদেনের সঙ্গে জড়িত রিস্ক কমাতে 2FA হিসাবে একটি ডায়নামিক ওয়ান-টাইম পাসওয়ার্ড (OTP) প্রয়োগ করবে।

x) কার্ড পেমেন্ট নিরাপত্তা বাড়াতে, ব্যাংক বা এনবিএফআই গ্রাহকদের পেমেন্ট কার্ডে করা যেকোনো লেনদেনের উৎস এবং পরিমাণসহ একটি এলার্টের মাধ্যমে কার্ডধারকদের অবিলম্বে অবহিত করবে।

xi) ব্যাংক বা এনবিএফআই জালিয়াতি শনাক্তকরণের ক্ষমতা বাড়ানোর জন্য কার্ডহোল্ডারদের দ্বারা সৃষ্ট ঝুঁকি অনুসারে লেনদেনের প্রকৃতি বা অন্য ঝুঁকির কারণগুলোকে বিবেচনায় নিয়া রিস্ক ম্যানেজমেন্ট প্যারামিটার তৈরি করবে।

xii) ব্যাংক বা এনবিএফআই কার্ডধারীর স্বাভাবিক কার্ড ব্যবহারের ধরণ থেকে উল্লেখযোগ্যভাবে বিচ্যুত আচরণ প্রদর্শনকারী লেনদেনগুলোর ফলোআপ করার উপায় বাস্তবায়ন করবে। ব্যাংক বা এনবিএফআই এই লেনদেনগুলো তদন্ত করবে এবং লেনদেন সম্পূর্ণ করার পূর্বে কার্ডধারকের অনুমোদন নিবে।

### ৫.৯.৪. মোবাইল ফিন্যান্সিয়াল সার্ভিসেস (Mobile Financial Service-MFS)

একটি অরক্ষিত পরিবেশে কাজ করার ঝুঁকিগুলো মোকাবিলা করতে মোবাইল লেনদেনের ওপর নিয়ন্ত্রণ প্রয়োজন। ব্যাংক বা এনবিএফআই নিরাপত্তা নিয়ন্ত্রণ, সিস্টেমের সহজলভ্যতা এবং পুনরুদ্ধারের ক্ষমতা সংক্রান্ত নীতি এমনভাবে প্রণয়ন

করবে, যেন তা এমএফএস অপারেশনের ক্ষেত্রে সম্ভাব্য ঝুঁকির মাত্রার সঙ্গে সামঞ্জস্যপূর্ণ থাকে।

i) সিকিউরিটি স্ট্যান্ডার্ড প্রদত্ত পরিষেবাগুলোর জটিলতার জন্য উপযুক্ত হবে।

ii) ব্যাংক বা এনবিএফআইগুলো ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ায় এমএফএস সেবার ধরনের সঙ্গে সম্পর্কিত ঝুঁকিগুলোকে স্পষ্টভাবে চিহ্নিত করবে।

iii) যদি না অন্যথায় নিয়ন্ত্রক সংস্থা দ্বারা বাধ্যতামূলক করা হয়, ঝুঁকি উপলব্ধির ওপর নির্ভর করে ব্যাংক বা এনবিএফআইগুলো এমএফএসেরর জন্য উপযুক্ত ঝুঁকি প্রশমন ব্যবস্থা বাস্তবায়িত করা হবে, যেমন লেনদেনের সীমা, লেনদেনের ফ্রিকোয়েন্সি সীমা, জালিয়াতি নিয়ন্ত্রণ, AML চেক, ইত্যাদি।

iv) ব্যাংক বা এনবিএফআই মোবাইল নেটওয়ার্ক অপারেটর (MNOs) এর সঙ্গে সিম প্রতিস্থাপন প্রক্রিয়া সম্পর্কে একটি চুক্তি সম্পাদন করবে—যার মধ্যে থাকবে, এমএফএস অ্যাকাউন্টে অবাঞ্ছিত লেনদেনের ঝুঁকি এড়াতে যথাযথ ব্যবস্থা নেওয়ার জন্য MNO কর্তৃক MFS কে পূর্ব বিজ্ঞপ্তি পাঠানো।

v) মোবাইলের মাধ্যমে ব্যাংকগুলো প্রদত্ত সেবাগুলোর জন্য নিয়ন্ত্রক সংস্থা দ্বারা নির্ধারিত লেনদেনের অথেনটিকেশন পদ্ধতি মেনে চলার জন্য নিরাপত্তা নীতি ও অনুশীলন প্রস্তুত করবে।

vi) ব্যাংক বা এনবিএফআই এমএফএস অপারেশনের পর্যায়ক্রমিক ঝুঁকি ব্যবস্থাপনা বিশ্লেষণ এবং নিরাপত্তা মূল্যায়ন পরিচালনা করবে এবং সেই অনুযায়ী যথাযথ ব্যবস্থা গ্রহণ করবে।

vii) ব্যাংক বা এনবিএফআই দেশের 'Regulatory Compliance'-এর প্রয়োজনীয়তার সঙ্গে সঙ্গতিপূর্ণ হবে।

viii) এই ধরনের মোবাইল আর্থিক পরিষেবাগুলোতে ব্যবহৃত নিরাপত্তা অনুশীলন, নির্দেশিকা, মেথড ও পদ্ধতিগুলোর যথাযথ ডকুমেন্টেশন বজায় রাখতে ও হালনাগাদ করতে হবে।

### ৫.১০. সেবা প্রদানকারী ব্যবস্থাপনা (Service Provider Management)

প্রবৃদ্ধির লক্ষ্যমাত্রা অর্জনে অংশীদার হিসাবে এবং খরচ কমানোর উদ্দেশ্যে বহিরাগত পরিষেবা প্রদানকারীদের (External Service Provider) ওপর ক্রমবর্ধমান বৃদ্ধি পাচ্ছে। আইসিটি আউটসোর্সিং অনেক ধরনের হতে পারে। আইসিটি আউটসোর্সিংয়ের সাধারণ কিছু উদাহরণ হলো, সিস্টেম ডেভেলপমেন্ট এবং রক্ষণাবেক্ষণ, ডিসি অপারেশনে সহায়তা, নেটওয়ার্ক অ্যাডমিনিস্ট্রেশন, দুর্যোগ পুনরুদ্ধার সেবা, অ্যাপ্লিকেশন হোস্টিং ও হার্ডওয়্যার রক্ষণাবেক্ষণ।

### ৫.১০.১. আউটসোর্সিং (Outsourcing)

আজকাল বাণিজ্যিক ব্যাংকগুলো তাদের বিভিন্ন আইসিটি পরিষেবা আউটসোর্স করে। এই ধরনের আউটসোর্সিং ব্যবস্থার চুক্তির মধ্যে সাধারণত কর্মক্ষমতার লক্ষ্য, পরিষেবার স্তর, প্রাপ্যতা, নির্ভরযোগ্যতা, মাপযোগ্যতা, কমপ্লায়েন্স, নিরীক্ষা, নিরাপত্তা, আকস্মিক (Contingency) পরিকল্পনা, দুর্যোগ পুনরুদ্ধারের ক্ষমতা ও ব্যাকআপ প্রক্রিয়াকরণ সুবিধা অন্তর্ভুক্ত থাকে।

i) পরিচালনা পর্ষদ ও সিনিয়র ব্যবস্থাপনা আইসিটি আউটসোর্সিংয়ের সঙ্গে সম্পর্কিত ঝুঁকিগুলো সম্পূর্ণরূপে বুঝতে সক্ষম হবে। একটি পরিষেবা প্রদানকারী নিয়োগ করার পূর্বে, এর কার্যকারিতা, সক্ষমতা, নির্ভরযোগ্যতা, ট্র্যাক রেকর্ড ও আর্থিক অবস্থান নির্ধারণে যথাযথ পরীক্ষা-নিরিক্ষা করতে হবে।

ii) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে, সমস্ত চুক্তিকারী পক্ষের ভূমিকা, সম্পর্ক, বাধ্যবাধকতা ও দায়িত্বগুলোকে চুক্তিপত্রে লিখিতভাবে সংযুক্ত করা হয়েছে।

iii) আউটসোর্সিং কার্যক্রম নিম্নলিখিত অনুশীলনের ওপর ভিত্তি করে মূল্যায়ন করা হবে—

ক) আউটসোর্সিং এর উদ্দেশ্য

খ) অর্থনৈতিক বাস্তবোপযোগিতা (Economic Viability)

গ) ঝুঁকি ও নিরাপত্তার উদ্বেগ (Risks and Security Concerns)।

iv) আইসিটি আউটসোর্সিং ব্যাংকের অভ্যন্তরীণ নিয়ন্ত্রণের কোনো দুর্বলতা বা অধঃপতন ঘটাবে না। ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে, পরিষেবা প্রদানকারীকে তার সুরক্ষা নীতি, পদ্ধতি এবং নিয়ন্ত্রণগুলো যেমন গ্রাহকের তথ্য, অবজেক্ট প্রোগ্রাম ও সোর্স কোডের গোপনীয়তা ও সুরক্ষা বজায় রাখতে যত্নবান থাকবে।

v) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে, পরিষেবা প্রদানকারী যথাযথ নিরাপত্তা নীতি, পদ্ধতি ও নিয়ন্ত্রণগুলো এমন কঠোরভাবে প্রয়োগ করবে যেমনটি তার নিজস্ব কার্যাবলির জন্য আশা করা যায়।

vi) ব্যাংক বা এনবিএফআই নিয়মিতভাবে পরিষেবা প্রদানকারীর নিরাপত্তা নীতি, পদ্ধতি এবং নিয়ন্ত্রণগুলো পর্যবেক্ষণ ও পর্যালোচনা করবে।

vii) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে, পরিষেবা প্রদানকারীকে একটি দুর্যোগ পুনরুদ্ধার কন্টিনজেন্সি ফ্রেমওয়ার্ক তৈরি ও প্রতিষ্ঠা করবে।

viii) ব্যাংক বা এনবিএফআই প্রযুক্তি পরিষেবা প্রদানকারীর অপ্রত্যাশিত সমস্যার কারণে সেবাসমূহের অপ্রাপ্ততা থেকে তাদের রক্ষা করার জন্য ক্রিটিক্যাল

আউটসোর্সড টেকনোলজি সার্ভিস সংক্রান্ত একটি আকস্মিক (Contingency) পরিকল্পনা তৈরি করবে। এর মধ্যে টার্মিনেশন প্ল্যান এবং এই ধরনের সহায়তা ও সেবার জন্য অতিরিক্ত বা বিকল্প প্রযুক্তি পরিষেবা প্রদানকারীদের শনাক্তকরণ অন্তর্ভুক্ত থাকতে পারে।

ix) ব্যাংক বা এনবিএফআই সমস্ত তৃতীয় পক্ষের পরিষেবাগুলোর জন্য একটি পরিষেবা ক্যাটালগ বজায় রাখবে যা প্রদত্ত প্রতিটি পরিষেবার হালনাগাদ তথ্য সংরক্ষণ করবে এবং পরিষেবা প্রদানকারীর নাম, পরিষেবার ধরন, এসএলএ (Service Level Arrangement বা SLA) মেয়াদ শেষ হওয়ার তারিখ, পরিষেবা গ্রহণকারী ব্যবস্থাপক, পরিষেবা রিপোর্টিং, জরুরি কন্টাক্ট পার্সন, শেষ এসএলএ পর্যালোচনার তারিখ, ইত্যাদি লিপিবদ্ধ করবে।

### ৫.১০.৩ সার্ভিস লেভেল চুক্তি (Service Level Agreement)

i) ব্যাংক বা এনবিএফআই ও ভেন্ডরদের মধ্যে একটি সার্ভিস লেবেল চুক্তি থাকতে হবে।

ii) ভেন্ডরের সঙ্গে বার্ষিক রক্ষণাবেক্ষণ চুক্তি (Annual Maintanence Contact বা AMC) সক্রিয় ও বর্তমানে কার্যকর থাকবে।

iii) SLA এবং AMC-এর জন্য উল্লেখযোগ্য বিবরণসহ একটি হালনাগাদ ড্যাশবোর্ড রাখা হবে।

iv) ব্যাংক বা এনবিএফআই নিশ্চিত করবে যে হার্ডওয়্যার সেবা প্রদানকারীর দ্বারা সার্ভিসিং/মেরামতের জন্য নেওয়া সরঞ্জামগুলোতে সংবেদনশীল সাম্প্রতিক তথ্য থাকবে না।

v) চুক্তিতে অন্তর্ভুক্ত প্রয়োজনীয়তা ও শর্তগুলোর মধ্যে অন্তর্ভুক্ত থাকবে কর্মক্ষমতার লক্ষ্যমাত্রা, পরিষেবার স্তর, প্রাপ্যতা, নির্ভরযোগ্যতা, মাপযোগ্যতা, সম্মতি, নিরীক্ষা, নিরাপত্তা, আকস্মিক পরিকল্পনা, দুর্যোগ পুনরুদ্ধারের ক্ষমতা ও ব্যাকআপ প্রক্রিয়াকরণ সুবিধা।

vi) তৃতীয় পক্ষের ভেন্ডরসহ সমস্ত পরিষেবা প্রদানকারীর সঙ্গে পরিষেবা চুক্তিতে অন্তর্ভুক্ত থাকবে :

ক) মূল্য নির্ধারণ (Pricing)
খ) পরিমাপযোগ্য পরিষেবা/চলক (measurable service/ deliverable)
গ) সময়/সূচি (Timing/Schedules)
ঘ) গোপনীয়তার ধারা (Confidentiality Clause)
ঙ) যোগাযোগের ব্যক্তির নাম (দৈনিক ক্রিয়াকলাপ ও সম্পর্কের স্তরে)
চ) Escalation Matrix সহ চুক্তিবদ্ধ পক্ষগুলোর ভূমিকা ও দায়িত্ব
ছ) রিনিউয়াল পিরিয়ড (renewal period)
জ) পরিবর্তন ধারা (modification clause)
ঝ) পরিষেবা রিপোর্টিংয়ের ফ্রিকোয়েন্সি (frequency of service reporting)
ঞ) টার্মিনেশন ধারা (termination clause)
ট) দণ্ড ধারা (penalty clause)
ঠ) পরিষেবা সরবরাহকারীদের কর্মচারীর দায়, তৃতীয় পক্ষের দায় এবং সম্পর্কিত প্রতিকারসহ ওয়ারেন্টি (warranty)।
ড) ভৌগোলিক অবস্থানের ব্যাপ্তি (geographical location covered)
ঢ) হার্ডওয়্যার এবং সফটওয়্যারের মালিকানা
ণ) ডকুমেন্টেশন (যেমন পরিবর্তনের লগ, ইভেন্ট লগ পর্যালোচনা করার রেকর্ড)
ত) তথ্য পদ্ধতি নিরীক্ষা করার অধিকার (অভ্যন্তরীণ বা বাহ্যিক)।

## ৬. পিসিআই-ডিএসএস, বি.এস৭৭৯৯ এবং আইএসও ২৭০০০

### ৬.১. পিসিআই-ডিএসএস (PCI-DSS)

#### ৬.১.১ পিসিআই ডিএসএস কী?

পেমেন্ট কার্ড ইন্ডাস্ট্রি ডেটা সিকিউরিটি স্ট্যান্ডার্ড (পিসিআই ডিএসএস) হলো একটি প্রতিষ্ঠিত তথ্য নিরাপত্তা স্ট্যান্ডার্ড, যা ক্রেডিট কার্ডের তথ্য প্রক্রিয়াকরণ, ট্রান্সমিশন ও স্টোরেজের সঙ্গে জড়িত যেকোনো প্রতিষ্ঠানের ক্ষেত্রে প্রযোজ্য। একটি স্বাধীন সংস্থা, PCI Security Standard Council (PCI-DSS) দ্বারা তৈরি ও পর্যবেক্ষণ করা, 'পিসিআই ডিএসএস' পেমেন্ট কার্ড লেনদেনের নিরাপত্তা উন্নত করতে এবং ক্রেডিট কার্ড জালিয়াতি কমাতে ডিজাইন করা হয়েছে।

PCI-SSC ২০০৬ সালে পাঁচটি বৃহত্তম পেমেন্ট কার্ড ব্র্যান্ডের (ভিসা, মাস্টারকার্ড, আমেরিকান এক্সপ্রেস, ডিসকভার এবং জেসিবি) মধ্যে একটি যৌথ উদ্যোগ হিসাবে প্রতিষ্ঠিত হয়েছিল। এর লক্ষ্য ছিল ভোক্তা তথ্য সুরক্ষায় একটি পরিষ্কার ও আন্তঃপরিচালনাযোগ্য মান তৈরি করা। যদিও SSC কোনো কমপ্লায়েন্স নিজে প্রয়োগ করে না, PCI-DSS এখন ব্যাপকভাবে স্বীকৃত এবং আকার বা শিল্প নির্বিশেষে ক্রেডিট, ডেবিট বা নগদ কার্ডের তথ্য নিয়ে কাজ করে এমন সমস্ত সংস্থার জন্য প্রযোজ্য।

#### ৬.১.২. পিসিআই ডিসিসি সার্টিফিকেশন (PCI-DSS Certification)

পিসিআই সার্টিফিকেশন পিসিআই এসএসসি দ্বারা নির্ধারিত নিয়মের মাধ্যমে একটি সংস্থার ব্যবসায় কার্ড ডেটার নিরাপত্তা নিশ্চিত করে। এর মধ্যে রয়েছে বেশ কয়েকটি সাধারণভাবে পরিচিত সেরা অনুশীলন, যেমন:

১. ফায়ারওয়াল ইনস্টলেশন করা (Installation of Firewalls)

২. তথ্য ট্রান্সমিশনের সময় এনক্রিপশন করা (Encryption of Data transmission)
৩. অ্যান্টি-ভাইরাস সফ্টওয়্যার ব্যবহার করা (Use of anti-virus software)।

এছাড়াও ব্যবসায়িকদের অবশ্যই কার্ডহোল্ডারের ডেটা অ্যাক্সেস সীমাবদ্ধ (restricted) করতে হবে এবং নেটওয়ার্ক সংস্থানগুলোতে অ্যাক্সেস নিরীক্ষণ করতে হবে।

'পিসিআই-কমপ্লায়েন্ট' নিরাপত্তা গ্রাহকদের জানায় যে সংস্থার ব্যবসার সঙ্গে তাদের লেনদেন করা নিরাপদ। বিপরীতভাবে, একজন ব্যবসায়ীকে তার ডেটা নিরাপত্তার বিষয়টি গুরুত্ব সহকারে বোঝার জন্য আর্থিক ও রেপোটেশনাল ক্ষতি, যা নন-কমপ্লায়েন্স থেকে উৎপন্ন হয় সে সম্পর্কে তাকে ধারণা প্রদান করাই যথেষ্ট। একটি ডেটা ব্রিচ (data breach), যা গ্রাহকের সংবেদনশীল তথ্য প্রকাশ করে, তা এন্টারপ্রাইজের ওপর মারাত্মক দুর্নাম ছড়াতে পারে। একটি ডেটা ব্রিচের ফলে পেমেন্ট কার্ড প্রদানকারীর কাছ থেকে জরিমানা, মামলা, বিক্রি হ্রাস ও ব্যাপকভাবে সুনাম ক্ষতিগ্রস্ত হতে পারে।

ডেটা ব্রিচের পরে, একটি প্রতিষ্ঠানকে তার ক্রেডিট কার্ড লেনদেন বন্ধ করতে হতে পারে বা বর্তমান চার্জের চেয়ে বেশি চার্জ দিতে বাধ্য করা হতে পারে। PCI সিকিউরিটি পদ্ধতিতে বিনিয়োগ প্রতিষ্ঠানের অন্যান্য বাণিজ্য দিকও দূষিত (malicious) অনলাইন actors থেকে মুক্ত রাখতে সাহায্য করে।

### ৬.১.৩. পিসিআই ডিএসএস কমপ্লায়েন্স লেভেল (PCI-DSS Compliance Levels)

একটি ব্যবসায়িক প্রক্রিয়ার ক্রেডিট বা ডেবিট কার্ড লেনদেনের বার্ষিক সংখ্যার ওপর ভিত্তি করে PCI Compliance চারটি স্তরে বিভক্ত। শ্রেণিবিন্যাস স্তর নির্ধারণ করে যে একটি এন্টারপ্রাইজকে অনুগত থাকার জন্য কী করতে হবে।

লেভেল ১ : বার্ষিক ছয় মিলিয়নেরও বেশি রিয়েল-ওয়ার্ল্ড ক্রেডিট বা ডেবিট কার্ড লেনদেন প্রক্রিয়াজাতকারী প্রতিষ্ঠানের জন্য প্রযোজ্য। তাদের অবশ্যই বছরে একবার একটি অনুমোদিত পিসিআই অডিটর দ্বারা অভ্যন্তরীণ নিরীক্ষা করাতে হবে। এছাড়াও, ত্রৈমাসিকে একবার তাদের অবশ্যই একটি অনুমোদিত স্ক্যানিং ভেন্ডর (Approved Scanning Vendor ev ASV) দ্বারা পিসিআই স্ক্যান করে তা জমা দিতে হবে।

লেভেল ২ : বার্ষিক এক থেকে ৬ মিলিয়ন রিয়েল-ওয়ার্ল্ড ক্রেডিট বা ডেবিট কার্ড লেনদেন প্রক্রিয়াজাতকারী প্রতিষ্ঠানের জন্য প্রযোজ্য। তাদের একটি স্ব-মূল্যায়ন প্রশ্নাবলি (Self-Assessment Questionnaire-SAQ) ব্যবহার করে বছরে একবার একটি মূল্যায়ন সম্পূর্ণ করতে হবে। এছাড়া একটি ত্রৈমাসিক পিসিআই স্ক্যান প্রয়োজন হতে পারে।

লেভেল ৩ : বার্ষিক ২০,০০০ থেকে এক মিলিয়ন ই-কমার্স লেনদেন প্রক্রিয়াজাতকরণ প্রতিষ্ঠানের ক্ষেত্রে প্রযোজ্য। তাদের অবশ্যই প্রাসঙ্গিক SAQ ব্যবহার করে একটি বার্ষিক মূল্যায়ন সম্পূর্ণ করতে হবে। একটি ত্রৈমাসিক পিসিআই স্ক্যানও প্রয়োজন হতে পারে।

লেভেল ৪ : বার্ষিক ২০,০০০-এর কম ই-কমার্স লেনদেন প্রক্রিয়াজাতকারী বা যারা এক মিলিয়ন পর্যন্ত রিয়েল-ওয়ার্ল্ড বাস্তব-বিশ্ব লেনদেন প্রক্রিয়া করে তেমন প্রতিষ্ঠানের জন্য প্রযোজ্য। প্রাসঙ্গিক SAQ ব্যবহার করে একটি বার্ষিক মূল্যায়ন অবশ্যই সম্পন্ন করতে হবে এবং একটি ত্রৈমাসিক পিসিআই স্ক্যানের প্রয়োজন হতে পারে।

### ৬.১.৪. পিসিআই ডিএসএস এর প্রয়োজনীয়তা (PCI-DSS requirements)

PCI-SSC কার্ডধারীর তথ্য পরিচালনা ও নিরাপদ নেটওয়ার্ক বজায় রাখতে ১২টি প্রয়োজনীয়তার রূপরেখা দিয়েছে। ছয়টি বৃহত্তর ভাগে বিভক্ত রূপরেখার প্রতিটি গোল (goal)-এর জন্যই প্রতিষ্ঠানকে কমপ্লায়েন্ট হতে হবে।

**ক) নিরাপদ নেটওয়ার্ক (Secure Network)**

১. একটি ফায়ারওয়ালের কনফিগারেশন অবশ্যই ইনস্টল ও রক্ষণাবেক্ষণ করতে হবে।
২. সিস্টেম পাসওয়ার্ডগুলো অবশ্যই অরিজিনাল হতে হবে (ভেন্ডর দ্বারা সরবরাহ করা নয়)

**খ) কার্ডধারীর ডেটা সুরক্ষিত করা (Secure Cardholder Data)**

৩. সংরক্ষিত কার্ডধারীর ডেটা অবশ্যই সুরক্ষিত থাকতে হবে।
৪. পাবলিক নেটওয়ার্ক জুড়ে কার্ডহোল্ডারের তথ্য স্থানান্তরের সময় অবশ্যই এনক্রিপ্ট করতে হবে।

**গ) দুর্বলতা ব্যবস্থাপনা (Vulnerability Management)**

৫. অ্যান্টি-ভাইরাস সফটওয়্যার ব্যবহার করতে হবে এবং নিয়মিত হালনাগাদ রাখতে হবে।

৬. সুরক্ষিত পদ্ধতি ও অ্যাপ্লিকেশন অবশ্যই তৈরি এবং রক্ষণাবেক্ষণ করতে হবে।

**ঘ) প্রবেশাধিকার নিয়ন্ত্রণ (Access Control)**

৭. কার্ডধারীর তথ্য অ্যাক্সেস অবশ্যই প্রতিষ্ঠানের Need-to-know ভিত্তিতে সীমাবদ্ধ থাকবে।

৮. কম্পিউটার অ্যাক্সেসসহ প্রত্যেক ব্যক্তিকে একটি অনন্য আইডি বরাদ্দ করতে হবে

৯. কার্ডধারীর ডেটাতে ফিজিক্যাল অ্যাক্সেস সীমাবদ্ধ থাকতে হবে।

**ঙ) নেটওয়ার্ক পর্যবেক্ষণ এবং পরীক্ষা (Network monitoring and testing)**

১০. কার্ডধারীর তথ্য ও নেটওয়ার্ক সম্পদে অ্যাক্সেস অবশ্যই শণাক্ত ও নিরীক্ষণ করতে হবে।

১১. নিরাপত্তা ব্যবস্থা ও প্রক্রিয়া নিয়মিত পরীক্ষা করতে হবে।

**চ) তথ্য নিরাপত্তা (Information Security)**

১২. তথ্য নিরাপত্তা সংক্রান্ত নীতিমালা বজায় রাখতে হবে।

### ৬.১.৫. পিসিআই ডিএসএস কমপ্লায়েন্স লেভেল বোঝা (Understanding PCI-DSS Compliance Levels)

চারটি পিসিআই ডিএসএস কমপ্লায়েন্স লেভেল রয়েছে। মার্চেন্টদের প্রতি বছর যে পরিমাণ লেনদেন প্রক্রিয়া করে তার ভিত্তিতে তাদেরকে শ্রেণিকরণ করা হয়। যেহেতু বৃহত্তর মার্চেন্টরা বেশি সংখ্যক ব্যক্তিগত লেনদেন করে থাকে, তাই তারা আরও বড় লক্ষ্যগুলোকে প্রতিনিধিত্ব করে এবং সম্ভাব্যভাবে আরও বেশি লোককে ঝুঁকির মুখে ফেলে। ফলস্বরূপ, উচ্চতর লেনদেন পরিমাণ বা মাত্রার জন্য কমপ্লায়েন্সের স্তরগুলো আরও কঠোর প্রয়োজনীয়তার সঙ্গে সঙ্গতিপূর্ণ।

| মার্চেন্ট স্তর | প্রয়োগযোগ্যতা (applicability) | সম্মতি প্রয়োজনীয়তা (Compliance Requirment) |
|---|---|---|
| ১ | প্রতি বছর ৬ মিলিয়নেরও বেশি পেমেন্ট কার্ড লেনদেন প্রক্রিয়াকরণ যে কোনো প্রতিষ্ঠান, সেইসঙ্গে SSC সদস্যদের দ্বারা বিশেষভাবে মনোনীত কিছু মার্চেন্ট। | ১. কমপ্লায়েন্সের রিপোর্ট প্রদান<br>২. দুর্বলতা (vulnerability) স্ক্যান (scan)<br>৩. কমপ্লায়েন্সের প্রত্যয়ন (attestation of compliance) |
| ২ | যে সমস্ত মার্চেন্ট প্রতি বছর ১ মিলিয়ন থেকে ৬ মিলিয়ন লেনদেন প্রক্রিয়া করে | ১.Self-Assessment Questionnaire (SAQ)<br>২. দুর্বলতা স্ক্যান<br>৩. কমপ্লায়েন্স প্রত্যয়ন |
| ৩ | যে সমস্ত মার্চেন্ট প্রতি বছর ২০,০০০ থেকে ১ মিলিয়ন ই-কমার্স লেনদেন প্রক্রিয়াজাতকরণ করে। | ১.স্ব-মূল্যায়ন প্রশ্নাবলি (SAQ)<br>২. দুর্বলতা স্ক্যান<br>৩. কমপ্লায়েন্স প্রত্যয়ন |
| ৪ | যে সমস্ত মার্চেন্টরা ২০,০০০ এরও কম ই-কমার্স লেনদেন বা প্রতি বছর ১ মিলিয়ন লেনদেন প্রক্রিয়াজাতকরণ করে। | ১.স্ব-মূল্যায়ন প্রশ্নাবলি (SAQ)<br>২. দুর্বলতা স্ক্যান<br>৩. কমপ্লায়েন্স প্রত্যয়ন। |

প্রতিটি কমপ্লায়েন্স স্তরে কেবল চারটি নির্দিষ্ট প্রয়োজনীয়তার কিছু অনুধাবন জড়িত। (১) স্ব-মূল্যায়ন প্রশ্নাবলি (SAQ), (২) দুর্বলতা (vulnerability) স্ক্যান, (৩) কমপ্লায়েন্সের সত্যতা (Attention of Compliance-AOC), এবং (৪) Report on Compliance (ROC)। তৃতীয় পক্ষের দ্বারা PCI-DSS মূল্যায়ন করার জন্য এই সমস্ত পদ্ধতি ব্যবহার করা হয়। এগুলো নিচে বর্ণিত হয়েছে—

**১. স্ব-মূল্যায়ন প্রশ্নাবলি (Self-Assessment Questionnaire-SAQ)**

এসএকিউতে বিভিন্ন হ্যাঁ বা না বোধক প্রশ্ন থাকে, যা কোনো সংস্থা পিসিআই ডিএসএসের সঙ্গে কমপ্লায়েন্স কি না তা মূল্যায়নের উদ্দেশ্যে করা হয়। এটি অবশ্যই সমস্ত মার্চেন্ট যাদের সম্মতি সম্পর্কিত (compliance related) কোনো প্রতিবেদনের প্রয়োজন নেই তাদের দ্বারা সম্পন্ন করতে হবে।

অনেক ধরনের প্রশ্নাবলি বিদ্যমান, তাই মার্চেন্ট ও পরিষেবা সরবরাহকারীদের অবশ্যই নির্ধারণ করতে হবে যে নির্দিষ্ট ফর্মগুলোর মধ্যে কোনটি SAQ শেষ করার পূর্বে তাদের জন্য প্রযোজ্য। এই নির্বাচনটি মূলত প্রতিষ্ঠান কীভাবে কার্ডের অর্থ প্রদান করে এবং প্রক্রিয়াজাত করে তার উপর ভিত্তি করে নির্ধারিত হয়। উদাহরণস্বরূপ, যে মার্চেন্টরা অনলাইন পেমেন্ট অ্যাপ্লিকেশনগুলো ব্যবহার করেন তবে কার্ডধারকের ডেটা তথ্য সঞ্চয় করে না তাদের SAQ-C পূরণ করা উচিত। প্রতিষ্ঠানগুলো পিসিআই ওয়েবসাইটে প্রাপ্ত রিসোর্সগুলো ব্যবহার করতে পারে যাতে তারা সঠিক এসএকিউ ফর্মটি বাছাই করতে পারে।

ব্যবহৃত নির্দিষ্ট প্রশ্নাবলির ওপর নির্ভর করে, এসএকিউ প্রায় ২০ থেকে ৩০০ টিরও বেশি প্রশ্নের আকারে তৈরি হতে পারে। মার্চেন্টদের পিসিআই ডিএসএসের সঙ্গে সম্মতি দিচ্ছে কি না তা সঠিকভাবে নির্ধারণ করার জন্য SAQ এর প্রশ্নগুলোর উত্তর দেওয়া উচিত।

### ২. দুর্বলতা স্ক্যান (Vulnerability Scan)

একটি দুর্বলতা স্ক্যান হলো মার্চেন্ট বা সার্ভিস প্রোভাইডারদের পাবলিক ইন্টারনেট ও গ্রাহকমুখী পেমেন্ট অ্যাপ্লিকেশন ও পোর্টালগুলোর বাহ্যিক স্ক্যান। এই স্ক্যানগুলো ব্যবহারিক স্তরে পিসিআই ডিএসএসের সঙ্গে কমপ্লায়েন্স মূল্যায়নে পিসিআই এসএসসি দ্বারা নিযুক্ত, অনুমোদিত স্ক্যানিং ভেন্ডর (Approved Scanning Vendor-ASV) দ্বারা সম্পাদিত হয়।

স্ক্যান করা সংস্থার পদ্ধতিগুলোতে কোনো দুর্বলতা বা তথ্য সুরক্ষা ঝুঁকি শনাক্ত করতে এএসভিগুলো একটি রিমোট টুল ব্যবহার করে। এই স্ক্যানগুলো অবশ্যই ত্রৈমাসিক ভিত্তিতে সম্পাদন করা উচিত (প্রতি ৯০ দিনে ১ বার)।

প্রযোজ্য কমপ্লায়েন্স স্তর নির্বিশেষে প্রায় সমস্ত মার্চেন্টকে অবশ্যই একটি স্ক্যান করতে হবে। কিন্তু কিছু মার্চেন্ট যারা এসএকিউ সম্পন্ন করেছে, তারা উপযুক্ত এসএকিউ ফর্মটি করা থেকে একই উপ-শ্রেণিকরণের ওপর ভিত্তি করে ছাড় পেতে পারে। বিশেষত, SAQ A-EP, B-IP, C and D (মার্চেন্ট বা পরিষেবা সরবরাহকারী) এর জন্য যোগ্যতা অর্জনকারী সংস্থাগুলো সমস্তই দুর্বলতা স্ক্যানের প্রয়োজনীয়তা পাস করতে বাধ্য। কিন্তু SAQ A,B, C-VT এবং PEPE-HW এর ক্ষেত্রে প্রয়োজন নেই।

### ৩. সম্মতির সত্যতা (Attestation of Compliance-AOC)

কমপ্লায়েন্স স্তর নির্বিশেষে পিসিআই ডিএসএস মেনে চলতে ইচ্ছুক সমস্ত মার্চেন্টদের জন্য AOC প্রযোজ্য। এই ডকুমেন্টটি মার্চেন্ট বা সার্ভিস প্রোভাইডার দ্বারা স্বাক্ষরিত ও সংরক্ষিত করা হয় যদি তারা তাদের নিজস্ব Questionnaire পূর্ণ করে থাকে। Report on Compliance-এর প্রয়োজন আছে এমন মার্চেন্টদের ক্ষেত্রে কোনও মূল্যায়নকারী দ্বারা পূর্ন করা হয়।

প্রতিটি ধরনের SAQ ফর্মের জন্য AOC-এর একটি সংস্করণ রয়েছে। উদাহরণস্বরূপ, একটি এসএকিউ 'এ' ডকুমেন্টের জন্য সংশ্লিষ্ট AOC 'A' নথিটি ব্যবহার করা উচিত।

এওসি হলো পিসিআই ডিএসএস মূল্যায়নের চূড়ান্ত ফলাফলের ঘোষণা। নথিটি শেষ পর্যন্ত পিসিআই ডিএসএস কমপ্লায়েন্সের প্রমাণ হিসাবে কাজ করে।

### ৪. কমপ্লায়েন্সের প্রতিবেদন (Report on Compliance-ROC)

SAQ-এর বিপরীতে, একটি ROC মার্চেন্টের পরিবর্তে QSA (Qualified Security Assessor) দ্বারা সম্পন্ন করা হয়। স্ক্যানিং ভেন্ডরের মতোন কিউএসএগুলো, পিসিআই ডিএসএস কমপ্লায়েন্সকে স্বাধীনভাবে মূল্যায়ন করতে পিসিআই এসসিসি দ্বারা অনুমোদিত একটি তৃতীয় পক্ষ সংস্থা।

সবশেষে, কিউএসএ সরাসরি মূল্যায়নের জন্য মার্চেন্ট ব্যাংকে প্রতিবেদনটি জমা দেয়। আরওসিগুলো কেবল বৃহত্তম, সর্বোচ্চ ঝুঁকিপূর্ণ মার্চেন্ট এবং বিক্রেতাদের জন্য প্রয়োজন। (তথ্যসূত্র : ইম্পিভা ওয়েবসাইট ও ট্যালেন্ট ওয়েবসাইট)

## ৬.২. বিএস৭৭৯৯

### ৬.২.১. বিএস ৭৭৯৯ কী?

BS 7799 একটি ব্রিটিশ স্ট্যান্ডার্ড, যা তথ্য সুরক্ষা ব্যবস্থাপনা পদ্ধতি (ISMS) জন্য একটি 'Code of Best Practices' সংজ্ঞায়িত করে।

বিএস৭৭৯৯ একটি উন্মুক্ত কাঠামো যা সুরক্ষা উন্নত করতে আগ্রহী যে কোনো প্রতিষ্ঠানের জন্য প্রযোজ্য।

বিএস ৭৭৯৯ / আইএসও ১৭৭৯৯ স্ট্যান্ডার্ড দুটি অংশে লিখিত ও প্রকাশিত হয়েছে—

১) বিএস ৭৭৯৯ পার্ট-১ : তথ্য সুরক্ষা ব্যবস্থাপনায় অনুশীলন কোড হলো অ্যাপ্লিক্যাশনের দশটি ফিল্ড অনুসারে কোনো সংস্থার তথ্যের সুরক্ষা নিশ্চিত করার জন্য পরামর্শ ও সুপারিশযুক্ত নির্দেশনা।

২) বিএস ৭৭৯৯ পার্ট ২ : তথ্য সুরক্ষা ব্যবস্থাপনা হলো Information Security Management System (ISMS) প্রতিষ্ঠার লক্ষ্যে সুপারিশমালা প্রদানের জন্য নির্দেশনাসহ কিছু স্পেসিফিকেশন। নিরীক্ষণের সময়, এই ডকুমেন্টটি প্রশংসাপত্র প্রাপ্তির ক্ষেত্রে মূল্যায়ন গাইড হিসাবে কাজ করে।

### ৬.২.২. বিএস ৭৭৯৯ এর ইতিহাস

একশ বছরেরও বেশি সময় ধরে, ব্রিটিশ স্ট্যান্ডার্ড ইনস্টিটিউশন (বিএসআই) কার্যকর ও উচ্চমানের শিল্পের মান প্রতিষ্ঠার উদ্দেশ্যে গবেষণা করেছে। একটি সাধারণ তথ্য সুরক্ষা কাঠামো তৈরির জন্য শিল্প, সরকার এবং ব্যবসায়িক অনুরোধের প্রতিক্রিয়া হিসাবে ১৯৯০-এর দশকের শুরুতে বিএস ৭৭৯৯ তৈরি করা হয়েছিল। ১৯৯৫ সালে, বিএস৭৭৯৯ স্ট্যান্ডার্ডটি আনুষ্ঠানিকভাবে গৃহীত হয়েছিল।

বিএস ৭৭৯৯ স্ট্যান্ডার্ডের দ্বিতীয় সংস্করণ মে ১৯৯৯-এ প্রকাশের আগে চার বছর ধরে বহু উন্নতি অন্তর্ভুক্ত হয়। এই সময়কালে International Organization for Standardization (IOS) ব্রিটিশ ইনস্টিটিউট কর্তৃক প্রকাশিত কাজে আগ্রহী হতে শুরু করে।

২০০০ সালের ডিসেম্বরে, ISO বিএস ৭৭৯৯ এর প্রথম অংশটি গ্রহণ করে, যাহা আইএসও ১৭৭৯৯ হিসাবে পরিচিত হয়। সেপ্টেম্বর ২০০২ সালে, বিএস ৭৭৯৯ স্ট্যান্ডার্ডের দ্বিতীয় অংশের একটি সংশোধন করা হয়েছিল, যা অন্যান্য ম্যানেজমেন্ট স্ট্যান্ডার্ড যেমন আইএসও ৯০০১: ২০০০ এবং আইএসও ১৪০০১ : ১৯৯৬ এবং Organization for Economic Cooperation and Development (OECD) এর প্রিন্সিপালগুলোর সঙ্গে সামঞ্জস্য করার উদ্দেশ্যে করা হয়েছিল।

বর্তমানে বিএস ৭৭৯৯/আইএসও ১৭৭৯৯ কে সর্বশেষ উন্নয়নের শীর্ষস্থানে রাখার জন্য আন্তর্জাতিক পর্যায়ে পরামর্শ করা হচ্ছে।

### ৬.২.৩. বিএস৭৭৯৯ বনাম আইএসও১৭৭৯৯

বিএস৭৭৯৯ পার্ট ১ একটি আইএসও স্ট্যান্ডার্ড (আইএসও/আইইসি ১৭৭৯৯-২০০০) হিসাবে অনুমোদিত হয়েছে, তবে পার্ট ২ আইএসও স্ট্যান্ডার্ড হিসাবে অনুমোদিত হয়নি। অতএব, 'আইএসও ১৭৭৯৯' সর্বদা বিএস৭৭৯৯ পার্ট ১-এর ভিত্তিতে আন্তর্জাতিক মানকে বোঝায়। আইএসও ১৭৭৯৯ উন্নত সুরক্ষার জন্য অনুশীলনের একটি কোড, তবে প্রশংসাপত্র পাওয়ার জন্য এর নির্দিষ্ট কোন প্রয়োজনীয়তা নেই। সুতরাং একটি সংস্থা বিএস৭৭৯৯ (পার্ট ২) এর জন্য মূল্যায়ন ও প্রত্যয়িত হতে পারে, কিন্তু আইএসও ১৭৭৯৯ এর জন্য নয়।

### ৬.২.৪. কাকে মেনে চলতে হবে?

কারও মেনে চলার দরকার নেই। বিএস৭৭৯৯ হলো স্বেচ্ছায় অনুশীলনীয় বেস্ট প্রেক্টিস, যা একটি প্রতিষ্ঠান কতটা সুরক্ষিত হতে পারে তার পরিমাপ করে। কিছু সংস্থা তাদের সুরক্ষা নিয়ন্ত্রণগুলো সংজ্ঞায়িত করতে অন্যান্য স্ট্যান্ডার্ড ব্যবহার করে। তবে, বিএস ৭৭৯৯ এর আন্তর্জাতিক স্বীকৃতির কারণে এটি দিন দিন আরও গ্রহণযোগ্যতা অর্জন করছে।

### ৬.২.৫. বিএস৭৭৯৯ : পার্ট-১ : সিকিউরিটি ডোমেন, অবজেক্টিভ ও কন্ট্রোল

বিএস৭৭৯৯ দ্বারা নিয়ন্ত্রিত সিকিউরিটি কন্ট্রোল এর ১০টি ডোমেন, ৩৬টি অবজেকটিভ ও ১২৭ কন্ট্রোল রয়েছে। ১০টি ডোমেনের প্রতিটির সংক্ষিপ্ত বিবরণ নিচে দেওয়া হয়েছে :

#### ৬.২.৫.১. ডোমেন-১ : সিকিউরিটি পলিসি (Security Policy)

i) ইনফরমেশন সিকিউরিটি পলিসি (Information Security Policy):
একটি পলিসি ডকুমেন্ট প্রকাশ করতে হবে এবং সব কর্মচারীর এর বিষয় বা কাঠামো সম্পর্কে সচেতন করতে হবে। এই নীতিটি শীর্ষ ব্যবস্থাপনার দ্বারা অনুমোদিত হওয়া উচিত।

#### ৬.২.৫.২. ডোমেন-২ : সিকিউরিটি অরগানাইজেশন (Security Organization)

i) তথ্য সুরক্ষা অবকাঠামো (Information Security Infrastructure)
সংস্থার মধ্যে তথ্য সুরক্ষা বাস্তবায়ন শুরু ও নিয়ন্ত্রণ করতে ম্যানেজমেন্ট কাঠামো স্থাপন করতে হবে।

ii) তৃতীয় পক্ষের অ্যাক্সেসের সুরক্ষা (Security of third party access) :
সংস্থার তথ্য প্রক্রিয়াকরণ সুবিধাগুলোতে তৃতীয় পক্ষের অ্যাক্সেস নিয়ন্ত্রণ করা উচিত।

পর্যাপ্ত সিকিউরিটি ম্যানেজমেন্ট ব্যতীত তৃতীয়পক্ষকে বাহির থেকে অ্যাক্সেস প্রদান করলে সংস্থার ইনফরমেশন সিকিউরিটি প্রসেসিং কেন্দ্র ঝুঁকির মধ্যে পড়তে পারে। যখন কোনো তৃতীয় পক্ষকে বাহির থেকে সংস্থায় প্রবেশের জন্য সংযোগ স্থাপনের প্রয়োজন হয়, তখন নির্দিষ্ট নিয়ন্ত্রণের জন্য প্রয়োজনীয়তা শনাক্ত করতে ঝুঁকি মূল্যায়ন করা উচিত। এই ঝুঁকি মূল্যায়নটির সময় প্রয়োজনীয় অ্যাক্সেসের ধরন, তথ্যের মূল্য, তৃতীয় পক্ষের দ্বারা নেওয়া নিয়ন্ত্রণগুলো এবং এই প্রবেশের ফলে সংস্থার সিকিউরিটিতে কী প্রভাব পড়তে পারে, তা বিবেচনায় নেওয়া উচিত।
তৃতীয় পক্ষকে দেওয়া অ্যাক্সেসের ধরনটি বিশেষ গুরুত্বপূর্ণ। উদাহরণস্বরূপ, ফিজিক্যাল অ্যাক্সেসের ঝুঁকির থেকে নেটওয়ার্কের সর্বত্র অ্যাক্সেস প্রদানের ঝুঁকি সম্পূর্ণ আলাদা। বিভিন্ন ধরনের অ্যাক্সেস হলো—

ক) ফিজিক্যাল অ্যাক্সেস, উদা: অফিস, কম্পিউটার কক্ষ, ক্যাবিনেট ফাইল ইত্যাদিতে প্রবেশ।

খ) লজিক্যাল অ্যাক্সেস, উদা: কোনো সংস্থার ডাটাবেস, তথ্য পদ্ধতিতে প্রবেশ।

iii) আউটসোর্সিং (Outsourcing)

তথ্য প্রক্রিয়াকরণের দায়িত্ব যখন অন্য কোনো সংস্থা থেকে আউটসোর্স করা হয়, তখন তথ্যের সুরক্ষা কঠোরভাবে বজায় রাখা উচিত।

### ৬.২.৫.৩. ডোমেন-৩ : সম্পদ শ্রেণিবিন্যাস ও নিয়ন্ত্রণ (Asset Classification and Control)

i) সম্পদের জন্য জবাবদিহিতা (Accountability for assets)

সমস্ত প্রধান তথ্য সম্পদের জন্য দায়বদ্ধতা নির্ধারন করতে হবে এবং একজন মনোনীত মালিক থাকতে হবে। সংস্থা তার সমস্ত সম্পদের মূল্য ও প্রয়োজনীয়তার ওপর পূর্ণ জ্ঞান রাখবে। এই তথ্যের ভিত্তিতে একটি সংস্থা তথ্য পদ্ধতি সঙ্গে সম্পর্কিত সম্পদের সুরক্ষা দিতে পারবে। ইনফরমেশন সিস্টেমের সঙ্গে যুক্ত সম্পদের বর্ণনা নিম্নে দেওয়া হল—

ক) তথ্য সম্পদ (Information assets) : ডাটাবেস ও ডেটা ফাইল, সিস্টেম ডকুমেন্টেশন, ইউজার ম্যানুয়াল, প্রশিক্ষণ উপাদান, অপারেশনাল বা সহায়তা পদ্ধতি, কন্টিনিউয়িটি প্লান, ফল ব্যাক ব্যবস্থা, আর্কাইভের তথ্য।

খ) সফ্‌টওয়্যার সম্পদ (Software assets) : অ্যাপ্লিকেশন সফ্‌টওয়্যার, সিস্টেম সফ্‌টওয়্যার, ডেভেলপমেন্ট টুল ও ইউটিলিটি।

গ) ফিজিক্যাল সম্পদ (Physical assets) : কম্পিউটার সরঞ্জাম (প্রসেসর, মনিটর, ল্যাপটপ, মডেম), যোগাযোগ সরঞ্জাম (রাউটার, পিএবিএক্স, ফ্যাক্স মেশিন, আনচার মেশিন), ম্যাগনেটিক মিডিয়া (টেপ ও ডিস্ক), অন্যান্য টেকনিক্যাল সরঞ্জাম (বিদ্যুৎ সরবরাহ, এয়ার-কন্ডিশনার ইউনিট), আসবাবপত্র।

ঘ) সার্ভিসেস (Services): কম্পিউটিং এবং যোগাযোগ পরিষেবা, সাধারণ ইউটিলিটি (যেমন: হিটিং, আলো, শক্তি, শীতাতপনিয়ন্ত্রণ)।

### ৬.২.৫.৪. ডোমেন-৪ : পার্সোনাল সিকিউরিটি (Personal Security)

#### i) কাজের সংজ্ঞা এবং মানবসম্পদে সুরক্ষা (Security in job definition and resourcing)

নিয়োগের সময় অর্থাৎ জব ডেস্ক্রিপশন ও কন্টাক্ট তৈরির সময়ই সুরক্ষাকে সম্বোধন করা উচিত এবং কোনো ব্যক্তির কর্মকালীন সময়ে তা পর্যবেক্ষণ করা উচিত। ম্যানেজারদের নিশ্চিত হওয়া উচিত যে, জব ডেস্ক্রিপশনে সুরক্ষা সংক্রান্ত বিষয়াদি অন্তর্ভুক্ত করা হয়েছে।

সংস্থার ইনফরশেন প্রসেসিং সুবিধা ব্যবহার করে এমন কর্মিদের একটি গোপনীয়তা চুক্তিতে স্বাক্ষর করা উচিত। কর্মিদের সাধারণত তাদের চাকুরীর শর্ত হিসাবে এই জাতীয় চুক্তিতে স্বাক্ষর করা উচিত।

এজেন্সি কর্মি ও তৃতীয় পক্ষের ব্যবহারকারীদের যদি ইতোমধ্যে বিদ্যমান চুক্তি দ্বারা নিয়ন্ত্রিত না হয়, তবে তাদেরকে সংস্থার তথ্য প্রক্রিয়াকরণ সুবিধার সঙ্গে সংযোগের পূর্বে গোপনীয়তা চুক্তিতে স্বাক্ষর করতে হবে।

কর্মসংস্থান বা চুক্তির শর্তাদি পরিবর্তন করার সময় গোপনীয়তা চুক্তিগুলো পর্যালোচনা করা উচিত, বিশেষত যখন কর্মচারীরা সংস্থা ছেড়ে চলে যেতে চায় বা তাদের কন্ট্রাক্ট শেষ হয়ে যায়।

#### ii) ব্যবহারকারী প্রশিক্ষণ (User Training)

ব্যবহারকারীদের সুরক্ষা পদ্ধতি ও তথ্য প্রক্রিয়াকরণ সুবিধার ওপর সঠিক প্রশিক্ষণ দেওয়া উচিত।

### ৬.২.৫.৫. ডোমেন-৫ : ফিজিক্যাল ও এনভায়রনমেন্টাল সুরক্ষা (Physical and Environmental Security)

কী পরিমাণ ইনফরমেশন সার্ভিস প্রদান করা হয় ও সমর্থিত ব্যবসায়িক কার্যকলাপের সংবেদনশীলতা ও সমালোচনার ওপর ভিত্তি করে সংস্থা থেকে সংস্থায় ফিজিক্যাল সিকিউরিটি পরিবর্তনশীল হবে।

#### i) সুরক্ষিত স্থান (Secure Areas)

গুরুত্বপূর্ণ বা সংবেদনশীল ব্যবসায়িক তথ্য প্রক্রিয়া এবং তাদের সুবিধাগুলো সুরক্ষিত জায়গায় রাখা উচিত।

এই জাতীয় সুবিধাগুলো অননুমোদিত অ্যাক্সেস, ক্ষতি এবং হস্তক্ষেপ থেকে ফিজিক্যালভাবে সুরক্ষিত হওয়া উচিত। এগুলো উপযুক্ত প্রবেশ নিয়ন্ত্রণ ও সুরক্ষা বাধাসহ একটি সংজ্ঞায়িত সুরক্ষা প্রাচীর দ্বারা সুরক্ষিত স্থানে বসাতে হবে। প্রদত্ত সুরক্ষার মাত্রা, নির্ধারণ করা ঝুঁকি নির্ধারণের সঙ্গে সামঞ্জস্যপূর্ণ হওয়া উচিত। অননুমোদিত অ্যাক্সেস বা কাগজপত্র ও মিডিয়াতে ক্ষতির ঝুঁকি হ্রাস করতে একটি পরিষ্কার ডেস্ক ও পরিষ্কার স্ক্রিন নীতি (a clear desk and clear screen policy) তৈরি করতে হবে।

#### ii) সরঞ্জাম সুরক্ষা (Equipment Security)

সরঞ্জাম বিদ্যুৎ ব্যর্থতা বা অন্যান্য ইলেকট্রিক অসঙ্গতি থেকে সুরক্ষিত করা উচিত। পাওয়ার ও তথ্য বহন করার জন্য টেলিযোগাযোগ ক্যাবলিং কোনো রকম বাধা বা ক্ষতি থেকে রক্ষা করা উচিত।

কোনো সংস্থার তথ্য সরঞ্জামের অপরিকল্পিত ডিসপোজালের মাধ্যমে সংস্থার ডেটা-আপস (compromise) হতে পারে। এটি লক্ষ করা উচিত যে 'মুছে ফেলা' তথ্য স্টোরেজ মিডিয়া থেকে সহজেই পুনরুদ্ধার করা যেতে পারে, কারণ মুছে ফেলা অগত্যা তথ্য মুছে দেয় না। এমনকি বিশেষভাবে মুছা ডেটা বা ওভাররাইট করা ডেটাও বিশেষ সরঞ্জাম ব্যবহার করে পুনরুদ্ধার করা যেতে পারে। খুব উচ্চ পর্যায়ের সেনসেটিভ ডেটা ফিজিক্যালি ধ্বংস বা সুরক্ষিতভাবে ওভার রাইট করা উচিত, যা সাধারণ 'মুছুন' কার্যক্রম বা ফাংশন থেকে পৃথক।

স্টোরেজ মিডিয়া যেমন হার্ড ড্রাইভ ধ্বংস করার বা ফেলে দেওয়ার পূর্বে অবশ্যই চেক করে নিতে হবে যে, সংবেদনশীল ডেটা ও লাইসেন্সকৃত সফটওয়্যার মুছে ফেলা হয়েছে বা ওভার রাইট করা হয়েছে।

খুব সংবেদনশীল তথ্যযুক্ত ক্ষতিগ্রস্ত স্টোরেজ ডিভাইসগুলোর জন্য তথ্যগুলো বিলুপ্ত বা ধ্বংস, মেরামত বা বাতিল করা উচিত কি না, এই ধরনের নির্ধারণে ঝুঁকি মূল্যায়নের প্রয়োজন হতে পারে।

### ৬.২.৫.৬. ডোমেন-৬ : যোগাযোগ ও অপারেশন ম্যানেজমেন্ট (Communications and Operation Management)

তথ্য প্রক্রিয়াকরণ এবং যোগাযোগের সুবিধাগুলো ম্যানেজ ও পরিচালনা করার জন্য বিস্তৃতির পরিমাণ ও প্রসিডিয়রগুলোর আনুষ্ঠানিকতা নির্ভর করবে সংস্থার আকার, সরঞ্জামের ধরন ও ব্যবসায়িক অ্যাপ্লিকেশনগুলোর প্রকৃতি এবং সংবেদনশীলতার ওপর এবং তা সংস্থা থেকে সংস্থায় ভিন্ন হবে। উদাহরণস্বরূপ, একটি সংস্থা যাহা অত্যন্ত নির্ভরশীল ও বিশ্বস্ত একটি তথ্য পদ্ধতি ও নেটওয়ার্কিং প্রযুক্তির ব্যবহার করে থাকে সেটির ক্ষেত্রে অন্য একটি সংস্থা, যা এই জাতীয় প্রযুক্তির কম ব্যবহার করে এবং প্রযুক্তির উপর কম নির্ভরশীল, তার চেয়ে বেশি মাত্রায় সুরক্ষা প্রদান প্রয়োজন। নীতিগতভাবে একই সুরক্ষা প্রক্রিয়াগুলো প্রয়োগ করা উচিত, তবে উপযুক্ত বিশ্লেষণসাপেক্ষে।

#### i) কার্যক্রম পদ্ধতি ও দায়িত্ব (Operational Procedures and Responsibilities)

সমস্ত তথ্য প্রক্রিয়াকরণ সুবিধার ম্যানেজমেন্ট ও পরিচালনার জন্য প্রয়োজনীয় দায়িত্ব ও পদ্ধতিগুলো প্রতিষ্ঠিত করা উচিত।

এটি সমর্থন করার জন্য উপযুক্ত পরিচালনার নির্দেশাবলি (Appropriate Operating Instruction) ও ঘটনার প্রতিক্রিয়া পদ্ধতিগুলো (Incident Response Procedures) তৈরি করা উচিত। অবহেলা বা ইচ্ছাকৃতভাবে পদ্ধতি অপব্যবহারের ঝুঁকি হ্রাস করতে যেখানে প্রয়োজন, সেখানে বৈশিষ্ট্যগুলো পৃথকীকরণের নীতি প্রয়োগ করা উচিত।

এই জাতীয় পদ্ধতিগুলোর সঠিক ও সুরক্ষিত পরিচালনা নিশ্চিত করার লক্ষ্যে সমস্ত ইনফরমেশন প্রসেসিং সিস্টেমের জন্য প্রসেডিউর তৈরি ও রক্ষণাবেক্ষণ করা উচিত। সিস্টেম ডেভলপমেন্ট, রক্ষণাবেক্ষণ বা পরীক্ষার জন্য ডকুমেন্টেড প্রসিডিউর প্রস্তুত করা উচিত, বিশেষত যদি এর জন্য অন্যান্য সংস্থার সাহায্যের প্রয়োজন হয়, যেমন, কম্পিউটার অপারেশন। সমস্ত অপারেটিং প্রসিডিউরসমূহকে আনুষ্ঠানিক দলিল হিসাবে বিবেচনা করা উচিত, এর কোনো পরিবর্তন প্রয়োজন হলে তা অনুমোদিত ব্যবস্থাপনার দ্বারা অনুমোদিত হতে হবে। অপারেটিং প্রসিডিউরগুলো কমপক্ষে বছরে একবার আপডেট করা উচিত। পরিচালনা পদ্ধতির একটি উদ্দেশ্য হলো দৈনিক ক্রিয়াকলাপে ব্যবসায়িক আবেদনের জন্য তথ্য সুরক্ষা নীতি মেনে চলতে প্রয়োজনীয় বিধিগুলো নির্দিষ্ট করা। উদাহরণস্বরূপ, তথ্য সুরক্ষা নীতিটি নির্দিষ্ট করতে পারে যে নির্দিষ্ট সরঞ্জামগুলো অব্যবহৃত সময়ে একটি তালাবদ্ধ কক্ষে রাখতে হবে। অপারেটিং প্রসিডিউরে উল্লেখ থাকবে, কে তালাবদ্ধ করার জন্য দায়ী, কে কক্ষ খুলবে, কোথায় চাবি রাখা হবে এবং কখন কক্ষটি খোলা হবে।

#### দায়িত্ব পৃথকীকরণ (Segmentation of Duties)

দায়িত্ব পৃথকীকরণ, দুর্ঘটনাজনিত বা ইচ্ছাকৃত পদ্ধতি অপব্যবহারের ঝুঁকি হ্রাস করে। তাই তথ্য বা পরিষেবার অননুমোদিত পরিবর্তন বা অপব্যবহারের সুযোগ কমাতে, নির্দিষ্ট কিছু দায়িত্ব বা দায়িত্বের ক্ষেত্রগুলোর ব্যবস্থাপনা বা পরিবর্তনকে আলাদা করার বিষয়ে বিবেচনা করা উচিত। বিশেষত, এটি সুপারিশ করা হয় যে একই কর্মচারীরা নিম্নলিখিত কাজগুলো করবে না—

ক. ব্যবসায়িক সিস্টেমের ব্যবহারল
খ. ডেটা এন্ট্রি।
গ. কম্পিউটার অপারেশন।
ঘ. নেটওয়ার্ক ব্যবস্থাপনা।
ঙ. সিস্টেম এডমিনেস্ট্রেশন।
চ. সিস্টেম তৈরি ও রক্ষণাবেক্ষণ।
ছ. চেঞ্জ ম্যানেজমেন্ট।

#### ii) হাউজ কিপিং (Housekeeping)

ডেটা ব্যাকআপ নেওয়া এবং মাঝে মাঝে পরীক্ষা করা, যাতে সময় মতোন ডেটা পুনরুদ্ধার করা নিশ্চিত হওয়া যায়, ইভেন্ট ও ফল্ট লগ করা এবং যেখানে উপযুক্ত, সরঞ্জামের পরিবেশ পর্যবেক্ষণ করতে রুটিন প্রসিডিউরসমূহ স্থাপন করা উচিত।

### ৬.২.৫.৭. ডোমেন-৭ : অ্যাক্সেস নিয়ন্ত্রণ (Access Control)

i) অ্যাক্সেস নিয়ন্ত্রণে ব্যবসার শর্তাবলি (Business requirements for access control)

কম্পিউটার তথ্য ও নেটওয়ার্ক পরিষেবা এবং তথ্য অ্যাক্সেস করা ব্যবসার প্রয়োজনীয়তার ভিত্তিতে নিয়ন্ত্রণ করা উচিত। এ ক্ষেত্রে তথ্য প্রচার ও লাইসেন্সের নীতিগুলো বিবেচনা করা উচিত।

ii) ব্যবহারকারীর অ্যাক্সেস ব্যবস্থাপনা (User Access Management):

ইনফরমেশন সিস্টেম ও সার্ভিসে অ্যাক্সেসের অধিকার বরাদ্দ নিয়ন্ত্রণ করার জন্য ফরমাল প্রসিডিউর থাকা উচিত।

প্রসিডিউরগুলো এর ব্যবহারকারী কর্তৃক অ্যাক্সেসের জীবনচক্রের সমস্ত স্তরকে অন্তর্ভুক্ত করতে হবে, নতুন ব্যবহারকারীদের প্রাথমিক নিবন্ধন থেকে শুরু করে তাদের চূড়ান্ত পদবি পর্যন্ত যখন তাদের আর তথ্য পদ্ধতি ও পরিষেবাগুলোতে অ্যাক্সেসের প্রয়োজন নেই। যেখানে উপযুক্ত সেখানে Priviliged access rights, যা ব্যবহারকারীদের সিস্টেমে ওভাররাইট করার ক্ষমতা প্রদান করে, তা নিয়ন্ত্রণ করা উচিত।

iii) ব্যবহারকারীর দায়িত্ব (User responsibilities)

কার্যকর নিরাপত্তার জন্য অনুমোদিত ব্যবহারকারীদের সহযোগিতা অপরিহার্য। ব্যবহারকারীদের কার্যকর অ্যাক্সেস নিয়ন্ত্রণ বজায় রাখতে তাদের দায়িত্ব সম্পর্কে সচেতন করা উচিত, বিশেষত পাসওয়ার্ডের ব্যবহার ও ব্যবহারকারীর সরঞ্জামগুলোর নিরাপত্তা সম্পর্কিত। যেখানে উপযুক্ত, ঘটনাগুলোর ক্ষেত্রে তদন্তে সহায়তা করার উদ্দেশ্যে ব্যবহারকারীর অ্যাক্সেসের একটি নথি বজায় রাখা উচিত।

ব্যবহারকারীদের পাসওয়ার্ড নির্বাচন ও ব্যবহারে ভালো নিরাপত্তা নীতি অনুসরণ করা উচিত।

ব্যবহারকারীদের নিশ্চিত করা উচিত যে অনুপস্থিত (unattended) সরঞ্জামগুলো যথাযথ সুরক্ষিত রয়েছে। ব্যবহারকারী এলাকায় স্থাপন করা যন্ত্রপাতি, যেমন ওয়ার্ক স্টেশন বা ফাইল সার্ভার, একটি বর্ধিত সময়ের জন্য unattended থাকলে অননুমোদিত অ্যাক্সেস থেকে সুরক্ষার প্রয়োজন হতে পারে। সমস্ত ব্যবহারকারী ও ঠিকাদারদের নিরাপত্তার প্রয়োজনীয়তা ও unattended সরঞ্জামগুলো রক্ষা করার পদ্ধতি এবং এই জাতীয় সুরক্ষা বাস্তবায়নের জন্য তাদের দায়িত্ব সম্পর্কে সচেতন করা উচিত।

iv) নেটওয়ার্ক অ্যাক্সেস নিয়ন্ত্রণ (Network access control)

নেটওয়ার্ক সার্ভিসের সঙ্গে সংযোগগুলো নিয়ন্ত্রণ করা উচিত।

সংযুক্ত ব্যবহারকারী বা কম্পিউটার পরিষেবাগুলো অন্য কোনো নেটওয়ার্ক পরিষেবাগুলোর নিরাপত্তার সঙ্গে আপোস করে না তা নিশ্চিত করার জন্য এটি প্রয়োজনীয়। কন্ট্রোলগুলোর মধ্যে নিম্নলিখিত অন্তর্ভুক্ত থাকবে—

ক) নেটওয়ার্ক সার্ভিসগুলোর মধ্যে উপযুক্ত ইন্টারফেস।

খ) রিমোট ব্যবহারকারী এবং সরঞ্জামের জন্য উপযুক্ত অথেনটিকেশন প্রক্রিয়া।

গ) ইনফরমেশন সার্ভিসগুলোতে ব্যবহারকারীর অ্যাক্সেস নিয়ন্ত্রণ।

ব্যবহারকারীদের শুধু সেই সার্ভিসগুলোতে সরাসরি অ্যাক্সেস দেওয়া উচিত যেগুলো ব্যবহার করার জন্য তারা বিশেষভাবে অনুমোদিত হয়েছে। নেটওয়ার্ক এবং কম্পিউটার সেবাগুলো যেগুলো একজন ব্যবহারকারী বা একটি নির্দিষ্ট টার্মিনাল থেকে অ্যাক্সেস করতে পারে সেগুলো ব্যবসায়িক অ্যাক্সেস নিয়ন্ত্রণ নীতির সঙ্গে সামঞ্জস্যপূর্ণ হওয়া উচিত।

বড় নেটওয়ার্কগুলোকে পৃথক কাঠামোগত ও যৌক্তিক ডোমেনে বিভক্ত করার প্রয়োজন হতে পারে। নেটওয়ার্কগুলো ক্রমবর্ধমানভাবে প্রথাগত সাংগঠনিক সীমার বাইরে প্রসারিত হচ্ছে, কারণ ক্রমাগ্বয়ে ব্যবসায়িক অংশীদারিত্ব তৈরি হচ্ছে, ফলে তথ্য প্রক্রিয়াকরণ ও নেটওয়ার্কিং সুবিধাগুলোর আন্তঃসংযোগ বা ভাগ করে নেওয়ার প্রয়োজন হচ্ছে। এই ধরনের এক্সটেনশনগুলো ইতোমধ্যে বিদ্যমান তথ্য পদ্ধতিগুলোতে অননুমোদিত অ্যাক্সেসের ঝুঁকি বাড়িয়ে তুলতে পারে। ফলে অন্যান্য নেটওয়ার্ক ব্যবহারকারীদের থেকে এটির সুরক্ষার প্রয়োজন হতে পারে। এই ধরনের পরিস্থিতিতে, নেটওয়ার্কের মধ্যে নিয়ন্ত্রণের প্রবর্তন, তথ্য পরিষেবা, ব্যবহারকারী এবং তথ্য সিস্টেমের গ্রুপগুলোকে আলাদা করার কথা চিন্তা করা যেতে পারে।

সরকারি বা বেসরকারি নেটওয়ার্ক পরিষেবাগুলোর একটি বিস্তৃত পরিসর সহজলভ্য, যার মধ্যে কিছু Value-added সার্ভিস অফার করে। নেটওয়ার্ক সেবাগুলোর ইউনিক (সম্ভবত জটিল) নিরাপত্তা বৈশিষ্ট্য থাকতে পারে। নেটওয়ার্ক সেবা ব্যবহার করে এমন সংস্থাগুলোকে নিশ্চিত করা উচিত যে তাদের নেটওয়ার্ক প্রদানকারী, সমস্ত পরিষেবাগুলোর সুরক্ষা বৈশিষ্ট্যগুলোর একটি স্পষ্ট বিবরণ প্রদান করেছে এবং ব্যবসায়িক অ্যাপ্লিকেশনগুলোর গোপনীয়তা, অখণ্ডতা ও প্রাপ্যতার জন্য যথেষ্ট সুরক্ষা ব্যবস্থা গ্রহণ করেছে।

v) কম্পিউটার অ্যাক্সেস নিয়ন্ত্রণ (Computer access control):

কম্পিউটার সিস্টেমে অ্যাক্সেস নিয়ন্ত্রণ করতে হবে। এই ধরনের অ্যাক্সেস অনুমোদিত ব্যবহারকারীর মধ্যে সীমাবদ্ধ করা উচিত।

সমস্ত ব্যবহারকারীদের তাদের ব্যক্তিগত এবং একমাত্র ব্যবহারের জন্য ইউনিক আইডেন্টিফায়ার (ইউজার আইডি) থাকা উচিত, যাতে পরবর্তীতে কে

কাজটি করল তা শনাক্ত করা যায়। ব্যবহারকারীর আইডি ব্যবহারকারীর পদবীর কোনো ইঙ্গিত দিবে না, যেমন—ব্যবস্থাপক, পরিদর্শক।

vi) অ্যাপ্লিকেশন অ্যাক্সেস নিয়ন্ত্রণ (Application acess control)

অ্যাপ্লিকেশন সিস্টেম ও ডেটা অ্যাক্সেস নিয়ন্ত্রণে যৌক্তিক অ্যাক্সেস নিয়ন্ত্রণ ব্যবহার করা উচিত।

সফ্টওয়্যার ও ডেটায় যৌক্তিক অ্যাক্সেস অনুমোদিত ব্যবহারকারীদের জন্য সীমাবদ্ধ করা উচিত। অ্যাপ্লিকেশন সিস্টেমের উচিত :

ক) একটি সংজ্ঞায়িত ব্যবসায়িক অ্যাক্সেস নিয়ন্ত্রণ নীতি অনুসারে তথ্য ও অ্যাপ্লিকেশন সিস্টেম ক্রিয়াকলাপে ব্যবহারকারীর অ্যাক্সেস নিয়ন্ত্রণ করা;

খ) যে কোনো ইউটিলিটি ও অপারেটিং সিস্টেম সফ্টওয়্যারকে অননুমোদিত অ্যাক্সেস থেকে সুরক্ষা প্রদান করা যা সিস্টেম বা অ্যাপ্লিকেশনের কন্ট্রোলসমূহকে ওভাররাইট করতে সক্ষম।

গ) অন্যান্য পদ্ধতির নিরাপত্তা যার সঙ্গে তথ্য সম্পদ শেয়ার করা হয় তার সঙ্গে কোনো আপোস করবেন না।

ঘ) শুধু মালিক, অন্যান্য মনোনীত অনুমোদিত ব্যক্তি বা ব্যবহারকারীদের সংজ্ঞায়িত গোষ্ঠীকে তথ্যের অ্যাক্সেস প্রদান করতে হবে।

vii) পদ্ধতি অ্যাক্সেস ও ব্যবহার পর্যবেক্ষণ (Monitoring system access and use)

অ্যাক্সেস নীতি ও মানগুলোর সঙ্গে সামঞ্জস্যতা নিশ্চিত করতে সিস্টেমগুলো পর্যবেক্ষণ করা উচিত।

ভবিষ্যতে তদন্ত ও অ্যাক্সেস নিয়ন্ত্রণ পর্যবেক্ষণে সহায়তা করতে অডিট-লগ একটি নির্ধারিত সময়ের জন্য রাখা উচিত, যাহা ব্যতিক্রমসমূহ ও অন্যান্য নিরাপত্তা সম্পর্কিত ইভেন্টসমূহ রেকর্ড করে থাকে।

### ৬.২.৫.৮. ডোমেইন-৮ : সিস্টেম ডেভেলপমেন্ট ও রক্ষণাবেক্ষণ (Systems devlopement and maintenance)

i) পদ্ধতির নিরাপত্তা প্রয়োজনীয়তা (Security requirements of systems)

এর মধ্যে অবকাঠামো, ব্যবসায়িক অ্যাপ্লিকেশন ও ইউজার কর্তৃক তৈরি অ্যাপ্লিকেশনসমূহ অন্তর্ভুক্ত থাকবে। এছাড়াও কিছুক্ষেত্রে, বিজনেস প্রসেস তৈরি ও বাস্তবায়ন নিরাপত্তার ক্ষেত্রে অত্যন্ত গুরুত্বপূর্ণ। তথ্য ব্যবস্থার তৈরির পূর্বে নিরাপত্তার প্রয়োজনীয়তা চিহ্নিত করা ও সম্মত হওয়া উচিত।

ii) অ্যাপ্লিকেশন সিস্টেমে নিরাপত্তা (Security in Application System)

ইউজার কর্তৃক তৈরি অ্যাপ্লিকেশনসহ সব অ্যাপ্লিকেশন সিস্টেমের জন্য উপযুক্ত কন্ট্রোল ও অডিট-ট্রেইল তৈরি করা উচিত।

অত্যন্ত সংবেদনশীল ও মূল্যবান তথ্য সুরক্ষার জন্য ডেটা এনক্রিপশন বিবেচনা করা উচিত। এনক্রিপশন হলো ডেটাকে একটি দুর্বোধ্যাকারে রূপান্তরিত করার প্রক্রিয়া, যা চলাচলের সময় বা সংরক্ষরণের সময় এর গোপনীয়তা রক্ষা করে। এনক্রিপশন প্রক্রিয়াটি দুই ধরনের ক্রিপ্টোগ্রাফিক কৌশলগুলোর মধ্যে একটি ব্যবহার করে। এনক্রিপশন দ্বারা প্রদত্ত সুরক্ষার স্তর অন্তর্নিহিত ক্রিপ্টোগ্রাফিক অ্যালগরিদমের ক্ষমতা, কী (Key) স্পেসের আকার, কীর দৈর্ঘ্য ও কীর সুরক্ষিত ব্যবস্থাপনার ওপর নির্ভর করে।

### ৬.২.৫.৯. ডোমেইন-৯: ব্যবসার ধারাবাহিকতা ব্যবস্থাপনা (Business Continuity Management)

i) ব্যবসার ধারাবাহিকতা ব্যবস্থাপনার দিক (Assests of business continuity management):

'ব্যবসায়িক ধারাবাহিকতা ব্যবস্থাপনা', প্রতিরোধমূলক ও পুনরুদ্ধার ব্যবস্থার সংমিশ্রণের মাধ্যমে দুর্যোগ ও নিরাপত্তা ব্যর্থতার কারণে সৃষ্ট ক্ষয়ক্ষতি (যেমন প্রাকৃতিক দুর্যোগ, দুর্ঘটনা, সরঞ্জামের ব্যর্থতা ও ইচ্ছাকৃত কর্মের কারণে হতে পারে) হ্রাস করে।

বিপর্যয়, নিরাপত্তা ব্যর্থতা ও সেবা প্রদানে ব্যর্থতা ইত্যাদির পরিণতি বিশ্লেষণ করা উচিত। যথাসময়ে যেন গুরুত্বপূর্ণ প্রক্রিয়াগুলো পুনরুদ্ধার করা যায়, তা নিশ্চিত করতে Contingency Plan তৈরি ও বাস্তবায়ন করা হবে। অন্যান্য সমস্ত ব্যবস্থাপনা প্রক্রিয়ার এই ধরনের পরিকল্পনাগুলো সচরাচর বজায় রাখা ও অনুশীলন করা উচিত এবং কর্মীদের সদস্য, সরবরাহকারী ও ঠিকাদারদের কাছে তা গ্রহণযোগ্য হতে হবে।

'ব্যবসায়িক ধারাবাহিকতা পরিকল্পনার' মধ্যে ঝুঁকি শনাক্তকরণ ও হ্রাস করার ব্যবস্থা অন্তর্ভুক্ত থাকবে, কোনো দুর্ঘটনা ঘটলে তার ক্ষতি হ্রাস করার পদ্ধতি থাকবে এবং জরুরি অপারেশনগুলো যথাসময়ে চালু করা নিশ্চিত করবে।

প্রতিষ্ঠান জুড়ে ব্যবসার ধারাবাহিকতা তৈরি করা ও বজায় রাখতে একটি ম্যানেজড্ প্রক্রিয়া থাকা উচিত। প্রক্রিয়াটি 'ব্যবসার ধারাবাহিকতা ব্যবস্থাপনার' নিম্নলিখিত মূল উপাদানগুলোকে সমর্থন করবে—

ক) ব্যবসার ঝুঁকি সম্পর্কে বোঝা, গুরুত্বপূর্ণ ব্যবসায়িক প্রক্রিয়াগুলোর শনাক্তকরণ ও অগ্রাধিকারসহ ঝুঁকির সম্ভাবনা ও প্রভাব সম্বন্ধে জানা।

খ) ব্যবসার ওপর বিভিন্ন মাত্রার ঝুঁকির প্রভাব সম্বন্ধে বোঝা (এটি গুরুত্বপূর্ণ যে ছোট ঘটনা বা গুরুতর ঘটনা যা সংস্থার চলমান কার্যকারিতার জন্য হুমকিস্বরূপ

তার সমাধান খুঁজে পাওয়া সম্ভব) এবং প্রতিটি তথ্য পদ্ধতির জন্য ব্যবসায়িক উদ্দেশ্য ও অগ্রাধিকার তৈরি করা।

গ) নির্ধারিত ব্যবসায়িক উদ্দেশ্য ও অগ্রাধিকারের সঙ্গে সামঞ্জস্যপূর্ণ একটি 'ব্যবসায়িক ধারাবাহিকতা ব্যবস্থাপনার' পরিকল্পনা প্রণয়ন ও নথিভুক্তকরণ;

ঘ) সম্মত কৌশলের সঙ্গে সামঞ্জস্য রেখে 'ব্যবসায়িক ধারাবাহিকতা ব্যবস্থাপনার' পরিকল্পনা প্রণয়ন ও নথিভুক্তকরণ;

ঙ) এই স্বীকৃতির জন্য যে পরিকল্পনা ও প্রক্রিয়াগুলো স্থাপন করা হয়েছে তার জন্য নিয়মিত পরীক্ষা ও হালনাগাদ করা প্রয়োজন।

চ) এটি নিশ্চিত করা যে, ব্যবসার ধারাবাহিকতার ব্যবস্থাপনা এবং এটি অর্জনের প্রক্রিয়া, সংস্থার প্রক্রিয়া ও কাঠামোর সঙ্গে সামঞ্জস্যপূর্ন। প্রক্রিয়া ও প্রতিবেদনের সমন্বয়ের দায়িত্ব সংস্থার একজন উচ্চ পদের কর্মকর্তার ওপর দিতে হবে।

### ৬.৩.৫.১০. ডোমেইন ১০ : কমপ্লায়েন্স (Compliance)

i) আইনি প্রয়োজনীয়তার সঙ্গে সম্মতি (Compliance with legal requirments)

ইনফরমেশন সিস্টেমের নকশা, পরিচালনা, ব্যবহার ও ব্যবস্থাপনা অবশ্যই বিধিবদ্ধ, নিয়ন্ত্রক ও চুক্তিভিত্তিক নিরাপত্তা প্রয়োজনীয়তার বিষয়সমূহ মেনে চলবে।

সমস্ত প্রাসঙ্গিক বিধিবদ্ধ, নিয়ন্ত্রক ও চুক্তিগত প্রয়োজনীয়তাগুলো প্রতিটি ইনফরমেশন সিস্টেমের জন্য স্পষ্টভাবে সংজ্ঞায়িত ও নথিভুক্ত করা উচিত। এই প্রয়োজনীয়তাগুলো পূরণ করতে নির্দিষ্ট নিয়ন্ত্রণ ও ব্যক্তিগত দায়িত্ব একইভাবে সংজ্ঞায়িত ও নথিভুক্ত করা উচিত।

আইনি প্রয়োজনীয়তার বিষয়ে সংস্থার আইনি উপদেষ্টা বা উপযুক্ত কোন যোগ্য আইনি অনুশীলনকারীর কাছ থেকে পরামর্শ নেওয়া উচিত। আইনি প্রয়োজনীয়তা দেশভেদে ভিন্ন হতে পারে এবং এক দেশে তৈরি করা তথ্য যখন অন্য দেশে প্রেরণ করা হয় (যেমন ট্রান্স-বর্ডার তথ্য প্রবাহ) তখন তা জটিল হতে পারে।

ii) পদ্ধতি নিরীক্ষা বিবেচনা (System Audit Considerations)

অডিটের প্রয়োজনীয়তা ও পরিচালনা পদ্ধতি ব্যবসায়িক প্রক্রিয়ায় বাধার ঝুঁকি কমাতে জড়িত কার্যকলাপের সঙ্গে পরিকল্পিত ও সম্মত হওয়া উচিত। নিম্নলিখিতগুলো লক্ষ্য করা উচিত—

ক) নিরীক্ষা যথাযথ ব্যবস্থাপনার সঙ্গে সামঞ্জস্য হওয়া উচিত।

খ) নিরীক্ষার সুযোগ সম্মত ও নিয়ন্ত্রিত হওয়া উচিত।

গ) নিরীক্ষাসমূহ সফ্টওয়্যার ও তথ্যে কেবল পড়তে পারার মধ্যে সীমাবদ্ধ হওয়া উচিত।

ঘ) অন্যান্য ধরনের অ্যাক্সেসের (রিড-ওনলি ব্যতীত) মধ্যে সিস্টেম ফাইল কপি করা থাকতে পারে, তবে তা নিরীক্ষা সম্পূর্ণ হলে সঙ্গে সঙ্গে মুছে ফেলা উচিত।

ঙ) নিরীক্ষার সময় আইটি সংস্থানগুলো স্পষ্টভাবে চিহ্নিত ও সহজলভ্য করা উচিত।

চ) অতিরিক্ত প্রক্রিয়াকরণের প্রয়োজনীয়তা চিহ্নিত করা ও সম্মত হওয়া উচিত।

ছ) নিরীক্ষক কর্তৃক সমস্ত অ্যাক্সেস মনিটর করা উচিত এবং তা লগ করা উচিত।

জ) সমস্ত পদ্ধতি, প্রয়োজনীয়তা ও দায়িত্বগুলো নথিভুক্ত করা উচিত।

### ৬.২.৬. বিএস ৭৭৯৯: পার্ট-II: আইএসএমএস (ISMS) এবং সার্টিফিকেশন

#### ৬.২.৬.১. সম্মতি/প্রত্যয়ন প্রক্রিয়া (Compliance/Certification Process)

বিএস ৭৭৯৯ এর সঙ্গে কমপ্লায়েন্স করা একটি আনুষ্ঠানিক এবং কখনও কখনও জটিল প্রক্রিয়া। ব্রিটিশ স্ট্যান্ডার্ড ইন্সটিটিউট (বিএসআই) দ্বারা সংজ্ঞায়িত পদক্ষেপগুলো নিম্নরূপ—

ক) স্ট্যান্ডার্ড দ্বারা সংজ্ঞায়িত ব্যবস্থাপনা কাঠামো স্থাপন করা।

খ) বিএসআই আনুষ্ঠানিক মূল্যায়নের জন্য খরচ ও সময়সীমার একটি হিসাব প্রদান করবে।

গ) বিএসআইতে একটি আনুষ্ঠানিক আবেদন জমা দিতে হবে।

ঘ) বিএসআই প্রতিষ্ঠানের বিবৃত নিরাপত্তা ও ঝুঁকি নীতিগুলোর পর্যালোচনা করবে। এটি ব্যবস্থাপনা পদ্ধতির কোন দুর্বলতা চিহ্নিত করতে সাহায্য করবে, যা সমাধান করা প্রয়োজন।

ঙ) বিএসআই একটি অন-সাইট মূল্যায়ন পরিচালনা করবে।

চ) অডিট সফলভাবে সমাপ্ত হলে, একটি 'সার্টিফিকেট অব রেজিস্ট্রেশন' জারি করা হবে যা আইএসএমএস-এর প্রয়োজনীয়তা চিহ্নিত করে।

#### ৬.২.৬.২. আইএসএমএস (ISMS) কী?

'সংগঠনের তথ্য সুরক্ষা নীতি এবং উদ্দেশ্যগুলো প্রতিষ্ঠা করা এবং তারপরে এই উদ্দেশ্যগুলো পূরণ করা।'

একটি ইনফরমেশন সিকিউরিটি ম্যানেজমেন্ট সিস্টেম (আইএসএমএস) সংবেদনশীল তথ্য সুরক্ষার উদ্দেশ্যে একটি কাঠামোগত পদ্ধতি বর্ননা করে। এটি কর্মচারী, প্রক্রিয়া ও তথ্য পদ্ধতিকে অন্তর্ভুক্ত করে।

### ৬.৩. আইএসও ২৭০০১

আইএসও ২৭০০১ হলো আন্তর্জাতিক স্ট্যান্ডার্ড, যা একটি তথ্য নিরাপত্তা ব্যবস্থাপনা সিস্টেমের (ISMS) স্পেসিফিকেশন প্রদান করে। ISO ২৭০০১ একটি প্রযুক্তি এবং ভেন্ডর-নিরপেক্ষ স্ট্যান্ডার্ড যাহা আকার, প্রকার বা প্রকৃতি নির্বিশেষে সমস্ত সংস্থার জন্য প্রযোজ্য। স্ট্যান্ডার্ডটি ব্যয় কমিয়ে আন্তর্জাতিক সর্বোত্তম অনুশীলনের সঙ্গে সামঞ্জস্য রেখে সংস্থাগুলোকে তাদের তথ্য সুরক্ষা প্রক্রিয়া পরিচালনা করতে সহায়তা করে।

### ৬.৩.১. আইএসএমএস (ISMS) বাস্তবায়নের সুবিধা

১. তথ্যসমূহে সব ধরনের সুরক্ষা প্রদান করে।
২. সাইবার আক্রমণের প্রতিরোধ ক্ষমতা বাড়ায়।
৩. কেন্দ্রীয়ভাবে পরিচালিত কাঠামো প্রদান করে।
৪. সংগঠনব্যাপী সুরক্ষা প্রদান করে।
৫. ক্রমবর্ধমান নিরাপত্তা হুমকিতে সাড়া দিতে সাহায্য করে।
৬. তথ্য নিরাপত্তার সঙ্গে যুক্ত খরচ কমায়।
৭. তথ্যের গোপনীয়তা, প্রাপ্যতা ও অখণ্ডতা রক্ষা করে।
৮. কোম্পানির সুরক্ষা সংস্কৃতি উন্নত করে।

### ৬.৩.২. আইএসও ২৭০০১ এর ১৪টি ডোমেইন কী কী?

আইএসও ২৭০০১ এর ১৪টি ডোমেইন হলো—

১. তথ্য সুরক্ষা নীতি (Information Security Policies): এই বিভাগে নিয়ন্ত্রণগুলো বর্ণনা করে যে কীভাবে তথ্য সুরক্ষা নীতিগুলো পরিচালনা করতে হয়।

২. তথ্য সুরক্ষা সংস্থা (Organization of Information Security) : এই বিভাগের নিয়ন্ত্রণগুলো তার অভ্যন্তরীণ সংস্থাকে সংজ্ঞায়িত করে (যেমন, ভূমিকা, দায়িত্ব, ইত্যাদি) এবং তথ্য সুরক্ষার সাংগঠনিক দিকগুলো যেমন- প্রকল্প পরিচালনা, মোবাইল ডিভাইসের ব্যবহার ও টেলিওয়ার্কিং ইত্যাদি ব্যবহার করে তথ্য সুরক্ষার বাস্তবায়ন ও পরিচালনার জন্য একটি মৌলিক কাঠামো প্রদান করে।

৩. মানবসম্পদ নিরাপত্তা (Human resource security) : এই বিভাগের নিয়ন্ত্রণগুলো নিশ্চিত করে যে সংস্থার নিয়ন্ত্রণে থাকা লোকেদের নিয়োগ দেওয়া, প্রশিক্ষিত করা এবং নিরাপদ উপায়ে পরিচালিত করা হয়; এবং শাস্তিমূলক পদক্ষেপ গ্রহণের নীতি ও চুক্তি বাতিলের নীতিগুলোও সঠিকভাবে সংজ্ঞায়িত হয়।

৪. সম্পদ ব্যবস্থাপনা (Asset Management): এই বিভাগের নিয়ন্ত্রণগুলো নিশ্চিত করে যে তথ্য সুরক্ষা সংক্রান্ত সম্পদগুলো (যেমন, তথ্য, প্রক্রিয়াকরণ ডিভাইস, সংরক্ষণ ডিভাইস, ইত্যাদি) সঠিকভাবে চিহ্নিত করা হয়েছে, তাদের নিরাপত্তার জন্য দায়িত্বগুলো মনোনীত করা হয়েছে এবং কর্মীরা জানে যে কীভাবে সেগুলো পরিচালনা করতে হয়।

৫. অ্যাক্সেস নিয়ন্ত্রণ (Access Control) : এই বিভাগের নিয়ন্ত্রণগুলো প্রকৃত ব্যবসায়ের প্রয়োজন অনুসারে তথ্য এবং তথ্য সম্পদের অ্যাক্সেসকে সীমাবদ্ধ করে। এটা ফিজিক্যাল বা লজিক্যাল উভয় ধরনের অ্যাক্সেসের জন্য প্রযোজ্য।

৬. ক্রিপ্টোগ্রাফি (Cryptography) : এই বিভাগের নিয়ন্ত্রণগুলো গোপনীয়তা, সত্যতা, অথবা তথ্যের অখণ্ডতা রক্ষায় এনক্রিপশন সমাধানগুলোর সঠিক ব্যবহারের জন্য ভিত্তি প্রদান করে।

৭. ফিজিক্যাল ও পরিবেশগত নিরাপত্তা (Physical and environmental security) : এই বিভাগের নিয়ন্ত্রণগুলো ফিজিক্যাল এলাকায় অননুমোদিত প্রবেশ রোধ করে এবং মানব বা প্রাকৃতিক হস্তক্ষেপ দ্বারা আপোস করা থেকে সরঞ্জাম ও সুবিধাগুলোকে রক্ষা করে।

৮. অপারেশন নিরাপত্তা (Operation Security) : এই বিভাগে নিয়ন্ত্রণগুলো নিশ্চিত করে যে অপারেটিং সিস্টেম ও সফ্টওয়্যার সহ আইটি সিস্টেমগুলো নিরাপদ এবং ডেটা লস থেকে সুরক্ষিত। উপরন্তু, এই বিভাগের নিয়ন্ত্রণগুলোর মধ্যে থাকবে বিষয়গুলো নথিভুক্ত করা ও evidence তৈরি করা, মাঝে মাঝে দুর্বলতার যাচাইকরণ, এবং নিরীক্ষা কার্যকলাপগুলো যেন অপারেশনকে বাধাগ্রস্ত না করে তার জন্য সতর্কতা অবলম্বন করা।

৯. যোগাযোগ সুরক্ষা (Communication Security) : এই বিভাগে নিয়ন্ত্রণগুলো নেটওয়ার্ক অবকাঠামো ও পরিষেবাগুলোকে রক্ষা করে, সেইসঙ্গে তাদের মাধ্যমে ভ্রমণ করা তথ্যগুলোকেও রক্ষা করে।

১০. পদ্ধতি অধিগ্রহণ, উন্নয়ন এবং রক্ষণাবেক্ষণ (System acquisition, development and maintenance) : এই বিভাগের নিয়ন্ত্রণগুলো নিশ্চিত করে যে নতুন তথ্য পদ্ধতি কেনার সময় বা বিদ্যমানগুলো হালনাগাদ করার সময় তথ্য সুরক্ষা বিবেচনায় নেওয়া হয়েছে।

১১. সরবরাহকারীর সম্পর্ক (Supplier relationsship): এই বিভাগের নিয়ন্ত্রণগুলো নিশ্চিত করে যে সরবরাহকারী ও অংশীদারদের দ্বারা সম্পাদিত আউটসোর্স কার্যাবলি উপযুক্ত তথ্য সুরক্ষা নিয়ন্ত্রণগুলো ব্যবহার করে এবং তৃতীয়-পক্ষের নিরাপত্তা কর্মক্ষমতা কীভাবে নিরীক্ষণ করতে হয় তা বর্ণনা করে।

১২. তথ্য নিরাপত্তা ঘটনা ব্যবস্থাপনা (Information Security Incident Management) : এই বিভাগের নিয়ন্ত্রণগুলো নিরাপত্তা বিষয় ও ঘটনাগুলোর সঠিক যোগাযোগ ও পরিচালনা নিশ্চিত করতে একটি কাঠামো প্রদান করে, যাতে সেগুলো সময়মত সমাধান করা যায়। কীভাবে evidence সংরক্ষণ করতে হয় ও কীভাবে তাদের পুনরাবৃত্তি রোধ করতে ঘটনাগুলো থেকে শিখতে হয়, তাও এই বিভাগে সংজ্ঞায়িত হয়।

১৩. ব্যবসার ধারাবাহিকতা ব্যবস্থাপনার তথ্য নিরাপত্তার দিক (Information security aspects of business continuity management): এই বিভাগের নিয়ন্ত্রণগুলো, দুর্যোগের সময় তথ্য নিরাপত্তা ব্যবস্থাপনার ধারাবাহিকতা ও তথ্য পদ্ধতির প্রাপ্যতা নিশ্চিত করে।

১৪. সম্মতি (Compliance): এই বিভাগের নিয়ন্ত্রণগুলো আইনি, সংবিধিবদ্ধ, নিয়ন্ত্রক ও চুক্তি লঙ্ঘন প্রতিরোধ করতে একটি কাঠামো প্রদান করে। এবং তা আইএসও২৭০০১ মানদণ্ডের সংজ্ঞায়িত নীতি, পদ্ধতি ও প্রয়োজনীয়তা অনুসারে কার্যকর কিনা তা অডিট করে।

এই ডোমেনগুলো আমাদের দেখায় যে তথ্য সুরক্ষা পরিচালনা শুধু আইটি নিরাপত্তার (যেমন, ফায়ারওয়াল, অ্যান্টি-ভাইরাস, ইত্যাদি) সঙ্গে সম্পর্কিত নয় বরং প্রক্রিয়াগুলো পরিচালনা, আইনি সুরক্ষা, মানব সম্পদ পরিচালনা, কাঠামোগত সুরক্ষা, ইত্যাদির সাথেও সম্পর্কিত।

### ৬.৩.৩. আইএসও ২৭০০১ এ কয়টি নিয়ন্ত্রণ আছে?

আইএসও ২৭০০১ এর ওপরে তালিকাভুক্ত ১৪টি বিভাগে সংগঠিত ১১৪টি নিয়ন্ত্রণ রয়েছে।


### ৬.৩.৪. 'আইএসও ২৭০০১ প্রত্যয়িত' (ISO 27001 Certified) কী?

একটি কোম্পানি আইএসও ২৭০০১ সার্টিফিকেশনের জন্য একটি স্বীকৃত সার্টিফিকেশন সংস্থাকে সার্টিফিকেশন নিরীক্ষার জন্য আমন্ত্রণ জানাতে পারে। যদি নিরীক্ষা সফল হয়, তাহলে সংস্থাটি কোম্পানিকে আইএসও ২৭০০১ সার্টিফিকেট ইস্যু করতে পারে। এই প্রশংসাপত্রের অর্থ হবে যে কোম্পানিটি আইএসও ২৭০০১ স্ট্যান্ডার্ডের সাথে সম্পূর্ণরূপে কমপ্লায়েন্ট।

একজন ব্যক্তিও আইএসও ২৭০০১ প্রশিক্ষণের মাধ্যমে এবং পরীক্ষায় উত্তীর্ণ হয়ে আইএসও ২৭০০১ সার্টিফিকেশন পেতে পারেন। এই প্রশংসাপত্রের অর্থ হবে যে এই ব্যক্তি কোর্স চলাকালীন সময়ে উপযুক্ত দক্ষতা অর্জন করেছেন।

(রেফারেন্স: ২৭০০০.org)

## ৭. বাংলাদেশে আইনি কাঠামো

### ৭.১. সাইবার আইন (Cyber Law)

### ৭.১.১. সাইবার আইন কী?

সহজ উপায়ে, আমরা বলতে পারি যে সাইবার ক্রাইম একটি বেআইনি কাজ যেখানে কম্পিউটার একটি টুল বা টার্গেট বা উভয়ভাবেই ব্যবহৃত হয়। সাইবার ক্রাইমের সঙ্গে ক্রিমিনাল কার্যকলাপ জড়িত হতে পারে, যা ট্রেডিশনাল যেমন চুরি, জাল-জালিয়াতি (fraud), জালিয়াতি (forgeries), মানহানি ও অনিষ্টসাধন, যার সবগুলোই বাংলাদেশ দণ্ডবিধির অধীন।

কম্পিউটারের অপব্যবহার নতুন ধরনের অপরাধেরও জন্ম দিয়েছে, যা তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (আইসিটি আইন-২০০৬) দ্বারা বর্ণিত হয়েছে।

### ৭.১.২. সাইবার অপরাধ শ্রেণিকরণ

আমরা সাইবার অপরাধকে দুটি উপায়ে শ্রেণিবদ্ধ করতে পারি:

ক) লক্ষ্য হিসাবে কম্পিউটার : অন্য কম্পিউটারকে আক্রমণ করতে কম্পিউটার ব্যবহার করে যেমন হ্যাকিং, ভাইরাস আক্রমণ, DOS আক্রমণ ইত্যাদি।

খ) কম্পিউটারকে একটি অস্ত্র হিসেবে : একটি কম্পিউটার ব্যবহার করে বাস্তব-বিশ্বের অপরাধ সংঘটিত করা যেমন সাইবার সন্ত্রাস, IPR লঙ্ঘন, ক্রেডিট কার্ড জালিয়াতি, EFT পস জালিয়াতি, পর্নোগ্রাফি, ইত্যাদি।

সাইবার অপরাধ সাইবার আইন বা ইন্টারনেট আইন দ্বারা নিয়ন্ত্রিত হয়।

### ৭.১.৩. সাইবার অপরাধ কার্যক্রম (Cyber Crime Activities)

প্রযুক্তিগত অগ্রগতি অপরাধমূলক কার্যকলাপের জন্য নতুন সম্ভাবনা তৈরি করেছে, বিশেষ করে, সাইবার অপরাধ পরিচালনায় তথ্য-প্রযুক্তির অপরাধমূলক অপব্যবহার যেমন—

i) অননুমোদিত অ্যাক্সেস ও হ্যাকিং (Hacking)

অ্যাক্সেস মানে একটি সংস্থার কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কের লজিক্যাল, অরিথম্যাটিকাল বা মেমরি ফাংশনে অননুমোদিতভাবে প্রবেশ বা এদেরকে নির্দেশ দেওয়া বা এদের সঙ্গে যোগাযোগ করা।

অননুমোদিত অ্যাক্সেস তাই সঠিক মালিক বা কম্পিউটার, কম্পিউটার সিস্টেম, বা কম্পিউটার নেটওয়ার্কের দায়িত্বে থাকা ব্যক্তির অনুমতি ছাড়াই যে কোনো ধরনের অ্যাক্সেসকে বোঝায়।

একটি কম্পিউটার এবং/অথবা নেটওয়ার্কের প্রতিরোধ ভাঙার জন্য করণীয় প্রতিটি কাজই হ্যাকিং। হ্যাকাররা কম্পিউটারে আক্রমণ করার উদ্দেশ্যে কম্পিউটার প্রোগ্রাম লিখে বা তা ব্যবহার করে। তারা ধ্বংস করার ইচ্ছা থেকে এই কাজগুলো করে থাকে। কিছু হ্যাকার ব্যক্তিগত আর্থিক লাভের জন্য হ্যাক করে, যেমন ক্রেডিট কার্ডের তথ্য চুরি করা এবং বিভিন্ন ব্যাংক অ্যাকাউন্ট থেকে তাদের নিজস্ব অ্যাকাউন্টে অর্থ স্থানান্তর করে অর্থ উত্তোলন করা।

ওয়েব সার্ভার হ্যাক করে অন্য ব্যক্তির ওয়েবসাইটের নিয়ন্ত্রণ নেওয়াকে web hijacking বলে।

ii) ট্রোজান আক্রমণ (Trojan attack)

ইহা এমন একটি প্রোগ্রাম, যা দেখতে দরকারি মনে হবে কিন্তু এমন কিছু কাজ করে যা ক্ষতিকর। এই ধরণের কম্পিউটার প্রোগ্রামকে ট্রোজান বলা হয়। এদের মধ্যে ট্রোজান হর্স নামটি জনপ্রিয়।

**ট্রোজান দুটি অংশে আসে**, একটি গ্রাহক অংশ এবং অন্যটি সার্ভার অংশ। যখন ভিক্টিম (অজান্তে) তার সার্ভারটি চালায়, তখন আক্রমণকারী সার্ভারের সঙ্গে সংযোগ করতে 'গ্রাহক' অংশ ব্যবহার করে এবং ট্রোজান ব্যবহার শুরু করা হয়। TCP/IP প্রোটোকল হলো যোগাযোগের জন্য বহু ব্যবহৃত একটি প্রোটোকল, কিন্তু ট্রোজানের কিছু কার্যক্রম UDP প্রোটোকলও ব্যবহার করে।

iii) ভাইরাস ও ওয়ার্ম আক্রমণ (Virus and worm attack)

যে প্রোগ্রাম অন্য প্রোগ্রামকে সংক্রামিত করে, এবং নিজের অনুলিপি তৈরি করে অন্য প্রোগ্রামে তা ছড়িয়ে দেয়, তাকে ভাইরাস বলে।

যেসব প্রোগ্রাম ভাইরাসের মতো বৃদ্ধি পায়, কিন্তু কম্পিউটার থেকে কম্পিউটারে ছড়িয়ে পড়ে তাদেরকে ওয়ার্ম বলে।

iv) ই-মেইল সম্পর্কিত অপরাধ (E-mail related crimes)

ক. ইমেল স্পুফিং (email spoofing)

ইমেল স্পুফিং বলতে এমন একটি ইমেলকে বোঝায়, যা একটি উৎস থেকে প্রেরণ করা হয়েছে বলে মনে হয়, যদিও সেটি প্রকৃত পক্ষে অন্য উৎস থেকে প্রেরণ করা হয়েছে।

খ. ইমেল স্প্যামিং (email spamming):

ইমেল 'স্প্যামিং' বলতে হাজার হাজার ব্যবহারকারীকে একটি ইমেল পাঠানোকে বোঝায়—একটি চেইন লেটারের মতো।

গ. ইমেলের মাধ্যমে দূষিত কোড পাঠানো (Sending malicious codes through email)

ই-মেইলগুলোর সংযুক্তি হিসাবে ভাইরাস, ট্রোজান, ইত্যাদি পাঠানো হয় বা ইমেইলের সঙ্গে সংযুক্তি হিসাবে এমন একটি ওয়েবসাইটের লিঙ্ক পাঠানো হয় যা প্রবেশ করলে malicious কোড কম্পিউটারে ডাউনলোড হয়ে যায়।

ঘ. ইমেইল বোম্বিং : (email bombing)

ই-মেইল বোম্বিং হলো অপব্যবহারকারী দ্বারা বারবার একটি নির্দিষ্ট ঠিকানায় একটি অভিন্ন ইমেইল বার্তা প্রেরণ করা।

ঙ. হুমকিমূলক ইমেইল পাঠানো
চ. মানহানিকর ইমেইল পাঠানো
ছ. ইমেইল জালিয়াতি।

v) ডস আক্রমণ (Denial of Service-DOS attacks)

একটি কম্পিউটার সিস্টেম যে পরিমাণ রিকুয়েস্ট নিতে পারে তার চেয়ে অনেক বেশি রিকুয়েস্ট প্রেরণ করা। ফলে কম্পিউটার সিস্টেম নষ্ট হয়ে যায় এবং সত্যিকারের ব্যবহারকারীরা সেবা থেকে বঞ্চিত হন।

vi) পর্নোগ্রাফি

কম্পিউটার ব্যবহার করে উৎপাদিত পর্নোগ্রাফিক সামগ্রী এবং পর্নোগ্রাফিক ভিডিও, ছবি, লেখা, ইত্যাদি তৈরি করা এবং ইন্টারনেট ব্যবহার করে তা প্রেরণ করা ও ডাউনলোড করাসহ সকল প্রকার পর্নোগ্রাফিক সাইট এর অন্তর্ভুক্ত।

প্রাপ্তবয়স্কদের বিনোদন ইন্টারনেটে সবচেয়ে বড় শিল্প। বর্তমানে ৪২০ মিলিয়নেরও বেশি ব্যক্তিগত পর্নোগ্রাফিক ওয়েবপেজ রয়েছে।

vii) জালিয়াতি (Forgery)

অত্যাধুনিক কম্পিউটার, প্রিন্টার ও স্ক্যানার ব্যবহার করে জাল নোট, ডাক, রাজস্ব স্ট্যাম্প, মার্কশিট, ইত্যাদি জাল করা যেতে পারে।

এছাড়াও, কোন ব্যক্তির ছদ্মবেশ ধারণকে জালিয়াতি হিসাবে বিবেচিত হয়।

viii) আইপিআর লঙ্ঘন (IPR Violations)

এর মধ্যে রয়েছে সফটওয়্যার পাইরেসি, কপিরাইট লঙ্ঘন, ট্রেডমার্ক লঙ্ঘন, কম্পিউটার সোর্স কোড চুরি, পেটেন্ট লঙ্ঘন, ইত্যাদি।

ডোমেন নেইমস্ ও একটি ট্রেডমার্ক এবং ICANN-এর ডোমেন বিরোধ নিষ্পত্তি নীতি ও ট্রেডমার্ক আইনের অধীনে সুরক্ষিত।

সাইবার সন্ত্রাসীরা জনপ্রিয় সেবা প্রদানকারীর ডোমেনের অনুরূপ ডোমেন নাম নিবন্ধন করে থাকে যাতে তারা ঐ সমস্ত সংস্থার ব্যবহারকারীদের আকৃষ্ট ও তাদের থেকে সুবিধা পেতে পারে।

ix) সাইবার সন্ত্রাস (Cyber Terrorism)

সামরিক স্থাপনা, পাওয়ার প্ল্যান্ট, এয়ার ট্রাফিক কন্ট্রোল, ব্যাংক, ট্রেইল ট্রাফিক কন্ট্রোল ও টেলিযোগাযোগ নেটওয়ার্কের ওপর আক্রমন সাইবার সন্ত্রাসের সম্ভাব্য লক্ষ্য। অন্যান্য লক্ষ্যের মধ্যে রয়েছে—পুলিশ, চিকিৎসা, অগ্নি ও উদ্ধার পদ্ধতি, ইত্যাদি।

সাইবার সন্ত্রাস বিভিন্ন কারণে আধুনিক সন্ত্রাসীদের জন্য একটি আকর্ষণীয় বিকল্প।

১. এটি ট্রেডিশনাল সন্ত্রাসী পদ্ধতির তুলনায় সস্তা।
২. সাইবার সন্ত্রাস ট্রেডিশনাল সন্ত্রাসী পদ্ধতির চেয়ে আলাদা।
৩. লক্ষ্যের বৈচিত্র্য ও সংখ্যা প্রচুর।
৪. সাইবার সন্ত্রাসবাদ দূর থেকে পরিচালিত হতে পারে, এটি এমন একটি বৈশিষ্ট্য, যা সন্ত্রাসীদের কাছে বিশেষভাবে আকর্ষণীয়।
৫. সাইবার সন্ত্রাসবাদে বিপুলসংখ্যক মানুষকে সরাসরি প্রভাবিত করা যায়।

x) ব্যাংকিং/ক্রেডিট কার্ড সম্পর্কিত অপবাদ (Banking/Credit card related crimes) :

কর্পোরেট জগতে, ইন্টারনেট হ্যাকাররা গোপনীয় ব্যাংকিং ও আর্থিক তথ্যে অ্যাক্সেস পেতে একটি কোম্পানির নিরাপত্তার সঙ্গে আপস করার সুযোগ খুজতে থাকে।

চুরি হওয়া কার্ডের তথ্য বা জাল ক্রেডিট/ডেবিট কার্ডের ব্যবহার খুবই সাধারণ বিষয়।

ব্যাংকের কর্মচারীরা সমস্ত গ্রাহকের অ্যাকাউন্ট থেকে অল্প পরিমাণ অর্থ কেটে নিতে কম্পিউটার প্রোগ্রাম ব্যবহার করে এবং তা তাদের নিজস্ব অ্যাকাউন্টে যোগ করে, যা সালামি (Salami) নামেও পরিচিত।

xi) ই-কমার্স/বিনিয়োগ জালিয়াতি (e-commerce/Investment Fraud):

বিক্রয় ও বিনিয়োগ জালিয়াতি, এমন একটি প্রস্তাব যা বিনিয়োগ বা ঋণের জন্য মিথ্যা বা প্রতারণামূলক তথ্য ব্যবহার করে, অথবা জাল সিকিউরিটিজ ক্রয়, ব্যবহার বা বাণিজ্যের জন্য ব্যবহার করে।

ব্যক্তিদের দ্বারা অনলাইনে কেনা পণ্যদ্রব্য বা সেবাগুলো কখনই বিতরণ করা হয় না।

ইন্টারনেট নিলাম সাইটের মাধ্যমে বিক্রয়ের জন্য বিজ্ঞাপন দেওয়া পণ্যের ভুল উপস্থাপন বা ইন্টারনেট নিলাম সাইটের মাধ্যমে কেনা পণ্য সরবরাহ না করার জন্য দায়ী হলো জালিয়াতি।

বিনিয়োগকারীরা অস্বাভাবিকভাবে বেশি লাভের প্রতিশ্রুতি দিয়ে এই প্রতারণামূলক প্রকল্পে বিনিয়োগ করতে প্রলুব্ধ হয়।

xii) অবৈধ জিনিস বিক্রি (Sales of illegal articles) :

ওয়েবসাইট, নিলাম ওয়েবসাইট ও বুলেটিন বোর্ডে তথ্য প্রকাশ করে বা কেবল ইমেলে যোগাযোগ করে মাদকদ্রব্য, অস্ত্র, বন্যপ্রাণী, ইত্যাদি ক্রয়-বিক্রয় করা এই ধরনের অপরাধের অন্তর্গত।

xiii) অনলাইন জুয়া (Online gambling) :

বিদেশে সার্ভারে হোস্ট করা লক্ষ লক্ষ ওয়েবসাইট রয়েছে, যেগুলো অনলাইন জুয়া খেলার সুযোগ করে দেয়। প্রকৃতপক্ষে, এটা বিশ্বাস করা হয় যে এই ওয়েবসাইটগুলোর মধ্যে অনেকগুলো আসলে অর্থ পাচারের জন্য ব্যবহৃত হয়।

xiv) মানহানি (Defamation) :

মানহানি হলো কোনো স্বনামধন্য ব্যক্তির সুনামের ক্ষতি করার প্রয়াস।

কম্পিউটার এবং/অথবা ইন্টারনেটের সাহায্যে মানহানি ঘটলে সাইবার মানহানি ঘটে। যেমন কেউ যদি একটি ওয়েবসাইটে কারও সম্পর্কে মানহানিকর বিষয় প্রকাশ করে বা সেই ব্যক্তির সমস্ত বন্ধুদের কাছে মানহানিকর তথ্য সংবলিত ই-মেইল পাঠায় তখন তা সাইবার মানহানি বোঝায়। সাইবার মানহানিকে সাইবার স্মিয়ারিংও (Cyber smearing) বলা হয়।

xv) Identity Theft :

Identity theft আমেরিকার মতো দেশে দ্রুততম ক্রমবর্ধমান একটি অপরাধ।

Identity theft ঘটে, যখন কেউ চুরি বা জালিয়াতি করার জন্য অন্যের ব্যক্তিগত তথ্য তাদের অজান্তেই ব্যবহার করে।

Identity theft হলো অন্য ধরনের জালিয়াতি স্কিম তৈরি করার একটি মাধ্যম।

আমাদের দেশে একজনের (NID) ব্যবহার করে তার অজান্তে ব্যাংক অ্যাকাউন্ট খুলে তা জালিয়াতির কাজে ব্যবহার করা হয়। এটি একটি Identity theft।

xvi) তথ্য বিভ্রান্তি (Data diddling)

তথ্য বিভ্রান্তির মধ্যে একটি কম্পিউটারে ডেটা ইনপুট করার পূর্বে বা করার সময় তথ্য পরিবর্তন করা জড়িত।

অন্য কথায়, কোনো ব্যক্তি দ্বারা টাইপ করা তথ্য বা ডাটাবেস ও অ্যাপ্লিকেশনের প্রোগ্রামার বা কম্পিউটারে তথ্য সংরক্ষণ করার সঙ্গে জড়িত অন্য কোনো ব্যক্তি যেভাবে তথ্য প্রবেশ করায়, তা পরিবর্তন হয়ে যায়।

এটি প্রক্রিয়াকরণের আগে কিছু সময়ের জন্য স্বয়ংক্রিয়ভাবে আর্থিক তথ্য পরিবর্তন এবং তারপর মূল তথ্য পুনরুদ্ধার অন্তর্ভুক্ত থাকে।

xvii) ইন্টারনেট সময় চুরি (Theft of Internet Hours) :

ইন্টারনেট একজন অননুমোদিতভাবে ব্যবহার করে, কিন্তু প্রকৃত মালিক বিল পরিশোধ করে।

একটি প্রতিষ্ঠানের টেলিফোন সুইচবোর্ডে (পিবিএক্স) অ্যাক্সেস লাভ করার মাধ্যমে ব্যক্তি বা অপরাধী সংস্থাগুলো ডায়াল-ইন/ডায়াল-আউট সার্কিটগুলোতে অ্যাক্সেস পেতে পারে এবং তারপরে তাদের নিজস্ব কল করতে পারে বা তৃতীয় পক্ষের কাছে কল টাইম বিক্রি করতে পারে।

পরিষেবা চুরির অন্যগুলোর মধ্যে রয়েছে 'কলিং কার্ড' (calling card) এর তথ্যাদি অধিগ্রহণ করা এবং অন-সেলিং কলসমূহের জন্য কলিং কার্ড অ্যাকাউন্টে চার্জ করা এবং সঞ্চিত মূল্যের টেলিফোন কার্ডের নকল বা অবৈধ পুনঃপ্রোগ্রামিং।

xviii) কম্পিউটার সিস্টেমের চুরি (হার্ডওয়্যার)

এই ধরনের অপরাধের মধ্যে কম্পিউটার, কম্পিউটারের কিছু অংশ বা কম্পিউটারের সঙ্গে সংযুক্ত একটি যন্ত্রাংশ চুরি জড়িত।

xix) কম্পিউটার পদ্ধতিকে ফিজিক্যালি ক্ষতিগ্রস্ত করা :

শক, আগুন, বা অতিরিক্ত বৈদ্যুতিক সরবরাহ ইত্যাদির মাধ্যমে কম্পিউটার বা এর যন্ত্রাংশ ক্ষতিগ্রস্ত করা হয়।

xx) প্রাইভেসি ও গোপনীয়তার লঙ্ঘন (Breach of privacy and confidentiality):

**প্রাইভেসি (Privacy)**

প্রাইভেসী বলতে একজন ব্যক্তির অধিকারকে বোঝায় যা নির্ধারণ করে তিনি কখন, কীভাবে এবং কতটা তার ব্যক্তিগত তথ্য অন্যদের সঙ্গে শেয়ার করবেন।

প্রাইভেসির লঙ্ঘন মানে ব্যক্তিগত তথ্য যেমন মেডিকেল রেকর্ড, যৌন পছন্দ, আর্থিক অবস্থা ইত্যাদির অননুমোদিত ব্যবহার, বিতরণ বা প্রকাশ।

**গোপনীয়তা (Confidentiality)**

এর অর্থ অননুমোদিত বা অবাঞ্ছিত ব্যক্তিদের কাছে তথ্য প্রকাশ না করা।

ব্যক্তিগত তথ্য ছাড়াও কিছু অন্যান্য ধরনের তথ্যের সুরক্ষা দরকার, যা ব্যবসার জন্য গুরুত্বপূর্ণ এবং অন্য ব্যক্তির কাছে এই ধরনের তথ্য ফাঁস করা ব্যবসা বা ব্যক্তিদের ক্ষতির কারণ হতে পারে।

সাধারণত, এই ধরনের তথ্যের গোপনীয়তা রক্ষায় পার্টিসমূহ তথ্য শেয়ার করার সময় তথ্য পরিচালনার পদ্ধতি সম্পর্কে এবং তৃতীয় পক্ষের কাছে যেন এই ধরনের তথ্য প্রকাশ না করে বা এমনভাবে যেন ব্যবহার না করে যাতে এটি তৃতীয় পক্ষের কাছে প্রকাশ পেয়ে যায়—এসব অন্তর্ভুক্ত করে একটি চুক্তি তৈরি করে।

অনেক সময় পার্টি বা তাদের কর্মীরা আর্থিক লাভের জন্য এই জাতীয় মূল্যবান তথ্য ফাঁস করে এবং গোপনীয়তার চুক্তি লঙ্ঘনের কারণ হয়।

বিশেষ কৌশল, যেমন সামাজিক ইঞ্জিনিয়ারিং, সাধারণত গোপনীয় তথ্য পেতে ব্যবহৃত হয়।

## ৭.২. আইসিটি আইন (ICT Act)

### ৭.২.১. ভূমিকা

কম্পিউটার আবিষ্কার, ডিজিটাল প্রযুক্তি ও যোগাযোগ ব্যবস্থার উন্নতির পর আমাদের জীবনে নাটকীয় পরিবর্তন ঘটেছে। কম্পিউটারের সাহায্যে ব্যবসায়িক লেনদেন

করা হচ্ছে। তবে, আমাদের দেশে, আইনি কাঠামোর অভাবের কারণে লোকেরা ব্যবসা পরিচালনা করতে বা ইলেকট্রনিক আকারে লেনদেন করতে অনিচ্ছুক ছিল। অনেক আইনি বিধান কাগজভিত্তিক রেকর্ড এবং স্বাক্ষর বহনকারী নথিগুলোকে স্বীকৃতি দেয় এবং বিভিন্ন বিরোধের ক্ষেত্রে তাদের প্রমাণ হিসাবে গ্রহণযোগ্য করে তোলে। ইলেকট্রনিক আকারে লেনদেন প্রায়ই আদালতে স্বীকৃত ছিল না। অনেক আইনি নিয়ম কাগজের রেকর্ড ও নথি, স্বাক্ষরিত রেকর্ড, আসল রেকর্ড, ফিজিক্যাল চেক, মুখোমুখি সাক্ষাৎকার, ইত্যাদির অস্তিত্ব আমলে নেয়। যেহেতু আরও বেশি ক্রিয়াকলাপ প্রযুক্তিগত উপায়ে পরিচালিত হয়, এটি প্রমাণের জন্য আরও বেশি গুরুত্বপূর্ণ হয়ে ওঠে। এই ক্রিয়াকলাপগুলো তাদের থেকে প্রচলিত আইনি অধিকার ও বাধ্যবাধকতাগুলো প্রদর্শনে সহজলভ্য।

### ৭.২.২. আইসিটি আইন-২০০৬ এর প্রযোজ্য ফিল্ডসমূহ (Applicable fields of ICT Act-2006)

উপরোক্ত আলোচনার পরিপ্রেক্ষিতে, 'ইনফরমেশন ও কমিউনিকেশন টেকনোলজি আইন-২০০৬' নামে একটি আইন প্রণয়ন করা হয়, যাহা নিম্নবর্ণিত ক্ষেত্রে প্রযোজ্য—

- নেগোসিয়েবল ইনস্ট্রুমেন্ট (negotiable instrument)
- পাওয়ার অব অ্যাটর্নি তৈরি, বহাল রাখা ও বলবৎ রাখা (creation, performance & enforcement of power of attorney)
- ট্রাস্ট (Trust)
- উইল (Will)
- স্থাবর সম্পত্তি বা এর সঙ্গে সংশ্লিষ্ট কোনো কিছুর বিক্রি বা পরিবহনের জন্য কোনো চুক্তি (any contract for sale or conveyance of immovable property or any interest in such property)
- টাইটেল ডকোমেন্ট (Document of Title)
- সরকার কর্তৃক গ্যাজেট দ্বারা প্রকাশিত যে কোনো ধরনের ডকোমেন্ট বা লেনদেন।

### ৭.২.৩. অবজেক্টিভ (Objectives)

ইনফরমেশন ও কমিউনিকেশন টেকনোলজি আইন-২০০৬ এর মূল লক্ষ্যগুলো হল—

১) ই-কমার্স লেনদেনের বাধা দূর করা।
২) সুরক্ষিত ই-কমার্স লেনদেনের উদ্দেশ্যে আইনি ও ব্যবসায়ী অবকাঠামো তৈরি করা।
৩) সরকারি সংস্থাগুলোতে ইলেকট্রনিক ফাইলিং সুবিধা প্রদান।
৪) সরকারি অফিসসমূহ থেকে ইলেকট্রনিক রেকর্ডের দক্ষ ডেলিভারি নিশ্চিত করা।
৫) অশ্লীল ও মানহানিকর তথ্য ইলেকট্রনিক পদ্ধতিতে প্রচার থেকে আধুনিক তথ্যপ্রযুক্তি ব্যবস্থাকে মুক্ত রাখা।
৬) সাইবার অপরাধীদের জন্য ১০ বছরের কারাদণ্ড বা ১০ মিলিয়ন টাকা পর্যন্ত জরিমানা বা উভয়টি নিশ্চিত করা।
৭) পুলিশ ও অন্য কর্মকর্তাদের ক্ষমতা বৃদ্ধি করা।
৮) সাইবার অ্যাফিলিয়েট ট্রাইব্যুনাল তৈরি।

### ৭.২.৪. নির্বাচিত ধারাসমূহ

এক্টের কয়েকটি ধারা নিচে সংক্ষিপ্ত আকারে উপস্থাপন করা হল—

**ধারা-৫ : ডিজিটাল স্বাক্ষরের মাধ্যমে ইলেকট্রনিক রেকর্ডসমূহ অথেনটিক করা**

(১) সাব-ধারা (২) এর বিধান সাপেক্ষে, যে কোনো গ্রাহক তার ডিজিটাল স্বাক্ষর সংযুক্ত করে যে কোনো ইলেকট্রনিক রেকর্ড অনুমোদন করতে পারবেন।
(২) অপেন টেকনিক বা প্রতিষ্ঠিত সরঞ্জাম বা কৌশল ব্যবহার করে তৈরি ইলেকট্রনিক স্বাক্ষর প্রদান করে ইলেকট্রনিক রেকর্ডসমূহ অনুমোদন করা যাবে।

**ধারা-৬: ইলেক্ট্রনিক রেকর্ডগুলির আইনী স্বীকৃতি**

যেখানে কোনও আইন উল্লেখ করে যে, তথ্য বা অন্য কোনও বিষয় লিখিত বা মুদ্রিত আকারে থাকবে, তবে ইহা, এই জাতীয় আইনে থাকা সত্ত্বেও, এই ধরনের প্রয়োজনীয়তা পরিপূর্ণ হয়েছে বলে মনে করা হবে; যদি এই তথ্য বা বিষয়বস্তু:
(ক) ইলেকট্রনিক আকারে সরবরাহ করা হয়, এবং
(খ) প্রবেশযোগ্য, যাতে পরবর্তী নির্দেশনার জন্য তাহা ব্যবহার করা যায়।

**ধারা ৭. ইলেক্ট্রনিক স্বাক্ষরগুলোর আইনি স্বীকৃতি**

যেখানে কোনো আইন উল্লেখ করে যে তথ্য বা অন্য কোনো বিষয় বা কোনো নথি স্বাক্ষর করে স্বাক্ষরিত হওয়া উচিত বা যে কোনো ব্যক্তির স্বাক্ষর বহন করা উচিত, তবে, এই জাতীয় আইনে যাই থাকুন না কেন, এই জাতীয় প্রয়োজনীয়তা অর্জিত হয়েছে বলে মনে করা হবে, যদি এই জাতীয় তথ্য বা বিষয় সরকার কর্তৃক নির্ধারিত হতে পারে এমনভাবে সংযুক্ত একটি ডিজিটাল স্বাক্ষরের মাধ্যমে প্রমাণীকরণ করা হয়।

**ধারা-৮. সরকার এবং তার সংস্থাগুলোতে ইলেকট্রনিক নথি ও ডিজিটাল স্বাক্ষরের ব্যবহার**

যেখানে কোন আইনের প্রয়োজন যে—

(ক) কোনো ফর্ম, আবেদন, বা অন্য কোনো নথি কোনো অফিস, কর্তৃপক্ষ, সংস্থা, বা সংস্থার মালিকানাধীন বা নিয়ন্ত্রিত কোনো নির্দিষ্ট পদ্ধতিতে যথাযথ সরকারের কাছে দাখিল করতে হবে।

(খ) কোনো লাইসেন্স, অনুমতি, অনুমোদন, বা অনুমোদন প্রদান বা মঞ্জুরি যে নামেই ডাকা হোক না কেন, তাহা প্রদান করতে হবে।

(গ) একটি নির্দিষ্ট পদ্ধতিতে অর্থ গ্রহণ বা পেমেন্ট করতে হবে, তাহলে, আপাতত বলবৎ অন্য কোনো আইনে যা কিছু থাকুক না কেন, এই ধরনের প্রয়োজনীয়তা অর্জিত হয়েছে বলে গণ্য হবে, যদি এই ধরনের ফাইলিং, ইস্যু, অনুদান, রসিদ, বা অর্থ প্রদান, সরকার কর্তৃক নির্ধারিত ইলেকট্রনিক পদ্ধতিতে সংঘটিত করা হয়।

**ধারা-১৩. ইলেকট্রনিক নথির বৈশিষ্ট্য, স্বীকৃতি ও প্রেরণ**

একটি ইলেকট্রনিক রেকর্ডের মালিক হিসাবে অরিজিনেটর বোঝাবে—

(ক) যদি এটি অরিজিনেটর নিজেই প্রেরণ করেন।

(খ) সেই ইলেকট্রনিক রেকর্ডের ক্ষেত্রে অরিজিনেটরের পক্ষে কাজ করার ক্ষমতা প্রাপ্ত ব্যক্তি দ্বারা প্রেরিত হয়েছে।

(গ) অরিজিনেটর দ্বারা বা তার পক্ষে যে কেউ দ্বারা নির্মিত কম্পিউটার প্রোগ্রাম থেকে স্বয়ংক্রিয়ভাবে প্রেরিত হয়েছে।

**অধ্যায়-৫ : নিয়ন্ত্রক ও প্রত্যয়নকারী কর্তৃপক্ষ (Controller and Certifying Authorities)**

**ধারা-১৮. নিয়ন্ত্রক এবং অন্য কর্মকর্তাদের নিয়োগ**

(১) সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের উদ্দেশ্যে প্রত্যয়নকারী কর্তৃপক্ষের একজন নিয়ন্ত্রক নিয়োগ করতে পারে এবং একই বা পরবর্তী প্রজ্ঞাপন দ্বারা যেভাবে উপযুক্ত বলে মনে হয় তত সংখ্যক উপ-নিয়ন্ত্রক এবং সহকারী নিয়ন্ত্রক নিয়োগ করতে পারে।

**ধারা-১৯. নিয়ন্ত্রক নিম্নলিখিত সকল বা যেকোনো কাজ সম্পাদন করতে পারে, যথা—**

(ক) প্রত্যয়নকারী কর্তৃপক্ষের কার্যক্রমের ওপর তত্ত্বাবধান অনুশীলন করা।

(খ) প্রত্যয়নকারী কর্তৃপক্ষের সর্বজনীন কীগুলো (Key) প্রত্যয়িত করা।

(গ) প্রত্যয়নকারী কর্তৃপক্ষ কর্তৃক রক্ষণাবেক্ষণের জন্য মান নির্ধারণ করা।

(ঘ) প্রত্যয়নকারী কর্তৃপক্ষের কর্মচারীদের যে যোগ্যতা ও অভিজ্ঞতা থাকতে হবে তা উল্লেখ করা।

(ঙ) প্রত্যয়নকারী কর্তৃপক্ষ তাদের ব্যবসা পরিচালনা করবে এমন শর্তগুলো উল্লেখ করা।

(চ) লিখিত, মুদ্রিত, বা ভিজুয়াল উপাদান ও বিজ্ঞাপনের বিষয়বস্তু নির্দিষ্ট করা, যা একটি ডিজিটাল স্বাক্ষর প্রশংসাপত্র ও সরকারি অনুমতির ক্ষেত্রে বিতরণ বা ব্যবহার করা যেতে পারে।

(ছ) একটি ডিজিটাল স্বাক্ষর প্রশংসাপত্রের গঠন, বিষয়বস্তু ও সমস্যা উল্লেখ করা;

(জ) প্রত্যয়নকারী কর্তৃপক্ষের দ্বারা অ্যাকাউন্টগুলো যে ধরন ও পদ্ধতিতে রক্ষণাবেক্ষণ করা হবে তা উল্লেখ করা।

(ঝ) নিরীক্ষক নিয়োগের শর্তাবলি তৈরি করা ও পারিশ্রমিক নির্ধারণ করা।

(ঞ) প্রত্যয়নকারী কর্তৃপক্ষ দ্বারা এককভাবে বা যৌথভাবে অন্যান্য প্রত্যয়নকারী কর্তৃপক্ষের সঙ্গে একত্রে একটি ইলেকট্রনিক পদ্ধতি স্থাপন করা।

(ট) প্রত্যয়নকারী কর্তৃপক্ষের সঙ্গে গ্রাহক কীভাবে লেনদেন পরিচালনা করবে তা উল্লেখ করা।

(ঠ) প্রত্যয়নকারী কর্তৃপক্ষ এবং গ্রাহকদের মধ্যে স্বার্থের কোনো সমস্যা হলে তা সমাধান করা।

(ড) প্রত্যয়নকারী কর্তৃপক্ষের দায়িত্ব নির্ধারণ।

(ঢ) প্রত্যয়নকারী কর্তৃপক্ষের উদঘাটিত **নথি** সম্বলিত একটি ডাটাবেস তৈরি করা, যা জনসাধারণের কাছে প্রবেশযোগ্য হবে।

**ধারা-২০. বিদেশি প্রত্যয়নকারী কর্তৃপক্ষের স্বীকৃতি (Recognition of foreign Certifying Authorities)**

(১) প্রবিধান দ্বারা নির্দিষ্ট করা শর্তাবলি এবং বিধিনিষেধ সাপেক্ষে, নিয়ন্ত্রক সরকারের পূর্বানুমোদন সাপেক্ষে এবং সরকারি গেজেটে বিজ্ঞপ্তি দ্বারা, এই উদ্দেশ্যে কোনো বিদেশি প্রত্যয়নকারী কর্তৃপক্ষকে প্রত্যয়নকারী কর্তৃপক্ষ হিসাবে স্বীকৃতি দিতে পারেন। .

(২) যেখানে কোনো প্রত্যয়নকারী কর্তৃপক্ষ উপ-ধারা (১) এর অধীনে স্বীকৃত হয়, এই আইনের উদ্দেশ্যে এই ধরনের প্রত্যয়নকারী কর্তৃপক্ষ দ্বারা জারি করা ডিজিটাল স্বাক্ষর বৈধ হবে।

**ধারা-২২। ডিজিটাল স্বাক্ষর প্রশংসাপত্র প্রদানের লাইসেন্স/সনদ**

(১) ডিজিটাল স্বাক্ষর প্রশংসাপত্র ইস্যু করার লাইসেন্সের জন্য যেকোনো ব্যক্তি নিয়ন্ত্রকের কাছে একটি আবেদন করতে পারেন।

(২) কোনো লাইসেন্স জারি করা হবে না, যদি না আবেদনকারী যোগ্যতা, দক্ষতা, জনশক্তি, আর্থিক সংস্থান এবং অন্যান্য পরিকাঠামো সুবিধার ক্ষেত্রে এই ধরনের প্রয়োজনীয়তাগুলো পূরণ না করে, যা সরকার দ্বারা নির্ধারিত ডিজিটাল স্বাক্ষর প্রশংসাপত্র জারি করতে প্রয়োজনীয়।

(৩) এই ধারার অধীনে প্রদত্ত একটি লাইসেন্স,
(ক) সরকার কর্তৃক নির্ধারিত সময়ের জন্য বৈধ হবে;
(খ) হস্তান্তরযোগ্য বা উত্তরাধিকারযোগ্য নয়;

(গ) প্রবিধান দ্বারা নির্দিষ্ট হতে পারে এই ধরনের শর্তাবলি সাপেক্ষে প্রদেয়।

**ধারা-৩১. কিছু পদ্ধতি অনুসরণ করার জন্য প্রত্যয়নকারী কর্তৃপক্ষ**

প্রতিটি প্রত্যয়নকারী কর্তৃপক্ষ—

(ক) অনুপ্রবেশ ও অপব্যবহার থেকে নিরাপদ হার্ডওয়্যার, সফ্টওয়্যার এবং পদ্ধতি ব্যবহার করবেএ

(খ) এর পরিষেবাগুলোতে একটি যুক্তিসঙ্গত স্তরের নির্ভরযোগ্যতা প্রদান করবে যা উদ্দেশ্যমূলক কার্যক্রমগুলোর কার্য সম্পাদনের জন্য যুক্তিসঙ্গতভাবে উপযুক্তএ

(গ) ডিজিটাল স্বাক্ষরের গোপনীয়তা রক্ষা করা **এবং এটা** নিশ্চিত করতে নিরাপত্তা পদ্ধতি মেনে চলবে এবং

(ঘ) প্রবিধান দ্বারা নির্দিষ্ট করা যেতে পারে এই ধরনের অন্যান্য মান পালন করবে।

**ধারা-৩৬. ডিজিটাল স্বাক্ষর সার্টিফিকেট ইস্যু করতে প্রত্যয়নকারী কর্তৃপক্ষ**

(১) যে কোনো ব্যক্তি সরকার কর্তৃক নির্ধারিত ফর্মে ডিজিটাল স্বাক্ষর সার্টিফিকেট পেতে প্রত্যয়নকারী কর্তৃপক্ষের কাছে আবেদন করতে পারে।

(২) এই জাতীয় প্রতিটি আবেদনের সঙ্গে একটি সার্টিফিকেশন অনুশীলন বিবৃতি বা যেখানে এই জাতীয় কোনও বিবৃতি নেই সেখানে এমন বিবরণ সংবলিত একটি বিবৃতি, যা প্রবিধান দ্বারা নির্দিষ্ট করা রয়েছে, তা প্রদান করতে হবে।

(৩) উপ-ধারা (১) এর অধীনে একটি আবেদন প্রাপ্তির পরে, প্রত্যয়নকারী কর্তৃপক্ষ, সার্টিফিকেশন অনুশীলন বিবৃতি বা উপ-ধারার অধীন অন্যান্য বিবৃতি বিবেচনা করার পরে—

(৪) এবং উপযুক্ত মনে হলে অনুসন্ধান করার পরে, ডিজিটাল স্বাক্ষর প্রশংসাপত্র মঞ্জুর করতে পারে বা লিখিতভাবে কারণ নথিভুক্ত করে আবেদনটি প্রত্যাখ্যান করতে পারে।

তবে শর্ত থাকে যে কোনো ডিজিটাল স্বাক্ষর প্রশংসাপত্র মঞ্জুর করা হবে না যদি না প্রত্যয়নকারী কর্তৃপক্ষ সন্তুষ্ট হয় যে—

(ক) আবেদনকারীর কাছে ডিজিটাল স্বাক্ষর প্রশংসাপত্রে তালিকাভুক্ত পাবলিক কী-এর সঙ্গে সম্পর্কিত প্রাইভেট কী রয়েছে;

(খ) আবেদনকারীর কাছে একটি প্রাইভেট কী রয়েছে, যা একটি ডিজিটাল স্বাক্ষর তৈরি করতে সক্ষম;

(গ) সার্টিফিকেটে তালিকাভুক্ত পাবলিক কটি আবেদনকারীর কাছে থাকা প্রাইভেট কী দ্বারা একটি ডিজিটাল স্বাক্ষর যাচাই করতে ব্যবহার করা যেতে পারে।

**অধ্যায়-৬ : গ্রাহকদের কর্তব্য**

**ধারা-৪২. ডিজিটাল স্বাক্ষর প্রশংসাপত্র গ্রহণযোগ্যতা**

একজন গ্রাহক একটি ডিজিটাল স্বাক্ষর প্রশংসাপত্র গ্রহণ করেছেন বলে গণ্য হবেন যদি তিনি একটি ডিজিটাল স্বাক্ষর প্রশংসাপত্র প্রকাশ করেন বা প্রকাশের জন্য অনুমোদন করেন—

(ক) এক বা একাধিক ব্যক্তির কাছে;

(খ) একটি ভান্ডারে বা অন্যথায় যেকোনো উপায়ে ডিজিটাল স্বাক্ষর প্রশংসাপত্রে তার অনুমোদন প্রদর্শন করে।

**অধ্যায় ৮ : শাস্তি ও বিচার**

**ধারা-৫৪. কম্পিউটার, কম্পিউটার পদ্ধতি, ইত্যাদির ক্ষতির জন্য শাস্তি**

মালিকের বা কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কের দায়িত্বে নিয়োজিত অন্য কোনো ব্যক্তির অনুমতি ব্যতীত যদি কোনো ব্যক্তি—

(ক) এই ধরনের কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে প্রবেশ করে বা করার চেষ্টা করে।

(খ) কোনো অপসারণযোগ্য স্টোরেজ বা সংরক্ষিত তথ্যসহ এই ধরনের কম্পিউটার, কম্পিউটার সিস্টেম, বা কম্পিউটার নেটওয়ার্ক থেকে কোনো তথ্য, কম্পিউটার ডাটাবেস বা তথ্য ডাউনলোড, কপি বা নিষ্কাশন করে।

(গ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, বা কম্পিউটার নেটওয়ার্কে কোনো কম্পিউটার দূষক (contaminant) বা কম্পিউটার ভাইরাস প্রবর্তন বা প্রবর্তন করার কারণ ঘটায়।

(ঘ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক, ডেটা, কম্পিউটার ডাটাবেস, বা এই জাতীয় কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে রক্ষিত প্রোগ্রামের ক্ষতি বা নষ্ট হওয়ার কারণ হয়।

(ঙ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, বা কম্পিউটার নেটওয়ার্ক ব্যাহত বা বিঘ্নিত করে (disrupts or causes disruption)।

(চ) অনুমোদিত কোনো ব্যক্তিকে যে কোনো উপায়ে, কোনো কম্পিউটার, কম্পিউটার সিস্টেম, বা কম্পিউটার নেটওয়ার্ক-এ অ্যাক্সেসে বাধা দেয় বা বাধার কারণ হয়।

(ছ) এই আইন, এর অধীনে প্রণীত বিধি বা প্রবিধানের বিধান লঙ্ঘন করে কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে অ্যাক্সেসের সুবিধার্থে কোনো ব্যক্তিকে যে কোনো সহায়তা প্রদান করে।

(জ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, বা কম্পিউটার নেটওয়ার্কের টেম্পারিং করে বা হেরফের করে (by manipulating) একজন ব্যক্তির দ্বারা করণীয় সেবার চার্জ অন্য ব্যক্তির অ্যাকাউন্টে প্রেরণ করে।

তবে, তিনি দশ বছর পর্যন্ত কারাদণ্ডে বা অনধিক ১০ লাখ টাকা অর্থদণ্ডে বা উভয় দণ্ডে দণ্ডিত হবেন।

**ধারা-৫৫. কম্পিউটারের সোর্স ডকোমেন্টে টেম্পারিং করা**

কম্পিউটার, কম্পিউটার প্রোগ্রাম, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কের জন্য ব্যবহৃত কোনো কম্পিউটার সোর্স কোড যাহা আপাতত বলবৎ আইন দ্বারা রাখা বা রক্ষণাবেক্ষণ করা প্রয়োজন, তাহা যদি কেউ জ্ঞাতসারে বা ইচ্ছাকৃতভাবে গোপন করে, ধ্বংস করে, পরিবর্তন করে, অথবা ইচ্ছাকৃতভাবে বা জ্ঞাতসারে অন্যকে গোপন, ধ্বংস বা পরিবর্তন করতে সাহায্য করে, তিনি তিন বছর পর্যন্ত কারাদণ্ডে, বা অনধিক তিন লক্ষ টাকা অর্থদণ্ডে বা উভয় দণ্ডে দণ্ডিত হবেন।

**ধারা-৫৬. কম্পিউটার সিস্টেম দিয়ে হ্যাকিং**

(১) যে ব্যক্তি জনসাধারণের বা কোনো ব্যক্তির অন্যায়ভাবে ক্ষতি করে বা ক্ষতির কারন হয়, কম্পিউটারে থাকা কোনো তথ্য ধ্বংস বা মুছে ফেলে বা পরিবর্তন করে বা এর মূল্য বা উপযোগিতা হ্রাস করে, বা যেকোনো উপায়ে ক্ষতিকারকভাবে প্রভাবিত করে, তাহলে তিনি হ্যাকিং করেছেন বলে ধরা হবে।

(২) যে ব্যক্তি হ্যাকিং করে সে দশ বছর পর্যন্ত কারাদণ্ডে বা অনধিক এক কোটি টাকা অর্থদণ্ডে বা উভয় দণ্ডে দণ্ডিত হবে।

**অধ্যায়-৮ : পার্ট-২ : সাইবার রেগুলেশন আপিল ট্রাইব্যুনাল**

**ধারা-৬৮. সাইবার আপিল ট্রাইব্যুনাল প্রতিষ্ঠা**

(১) সরকার, প্রজ্ঞাপন দ্বারা, সাইবার রেগুলেশন আপিলেট ট্রাইব্যুনাল নামে পরিচিত এক বা একাধিক আপিল ট্রাইব্যুনাল প্রতিষ্ঠা করবে।

(২) সরকার উপধারা (১) এ উল্লিখিত বিজ্ঞপ্তিতে সাইবার আপিল ট্রাইব্যুনাল যে এখতিয়ার প্রয়োগ করতে পারে সেই বিষয়সমূহ উল্লেখ করবে।

## পর্যালোচনামূলক প্রশ্নাবলি

**1. Multiple Choice Questions (MCQ)**

i) Near Data Center (NDC) is built in ----- for quick start of operation in case of major or minor breakdown in Data Center (DC).

a) Same City b) Different City c) Same Seismic Zone d) Different Seismic Zone

ii) Which of the following is a major IT shutdown?

a) Database Corrupted b) Server non-functioning c) UPS is not working d) Cooling system is out of order

iii) Which of the following is a remedy for Application Server non-functioning?

a) Active-active clustering b) Network Load Balancing c) Redundant UPS d) Active-Standby System

iv) To prevent unauthorized use of cards in an e-commerce site, Card issuing bank deliver a ----- token to the cardholder for use during e-commerce transaction.

a) OTP b) 2FA c) POS d) ATM

v) Ransomware is a type of malicious software that block access to users in to their IT system unless a ----- is paid.

a) Dollar b) Bitcoin c) Ransom d) Taka

vi) A----- is first sent to many employees of a bank as attachment of a email narrating attractive offeres.

a) Hacker b) Database c) Router d) Malware

vii) Phishing is presenting a----.

a) fake email b) fake website c) fake credit card d) fake password

viii) Which of the following is not a crypto currency?

a) Bitcoin b) Ether c) Router d) Petr

**2. Fill in the gap(s)**

i) For the first time, IT professionals started protecting their database and network placing ------ on the network.

ii) To keep the data safe and available in case of any disaster, IT professionals built ----- and-----.

iii) Unsatisfied ----- may steal data and handover to the hackers.

iv) Duplicating a credit card by fraudster is called -----.

v) A---- card can prevent skimming of cards in ATM.

vi) Corrupted----- are engaged in POS skimming.

vii) DDoS attack is done by attackers to ---- a website.

viii) ---- system and---- system maintain balance in USD and are most vulnerable to hacking.

# সম্ভাব্য প্রশ্নাবলি

1. What is the difference between ICT Security and Cyber Security?
2. Why Data Centers are very important part of ICT risks?
3. Narrate Business Continuity Threats, Classify Business Discontinuity.
4. Describe different types of Internal Threats.
5. List different threats related to MFS and their remedies.
6. Describe ATM Skimming and POS Skimming? Where you can use the anti-skimming device?
7. What is ATM Jackpotting?
8. How fraud occurs in e-commerce?
9. Describe following cyber treats: DDos, Ransomeware and Malware.
10. What is hacking? How money is unauthorizedly transferred from the client's account by the Hackers?
11. Why Swift and Credit Card is in the risk of cyber treat in Bangladesh?
12. Do you think that Crypto-currency is threat? Why?
13. Put your suggestions to minimize ICT risk and Cyber Treats.
14. Differentiate between Security Standards and Regulations.
15. Name three popular Regulations.
16. Why Banks should acquire "Certification" on popular "Security Standards"?
17. Write ten important points covered in the guideline on "ICT Security for scheduled Banks and Financial Institutes" published by the Bangladesh Bank.
18. With respect to the "ICT Security of scheduled banks and financial institutes" published by the Bangladesh Bank, reply to the following:

a) Narrate the roles and responsibilities of Board of Directors.

b) Narrate the roles and responsibilities of of ICT Steering Committee.

c) Narrate the roles and responsibilities of ICT Security Committee.

d) What is ICT Risk Governance?

e) What do you know about Change Management?

f) What is Incident Management?

g) What is BYOD?

h) What do you mean by Physical Security of Data Center?

i) Why email management is important?

j) What is User Access Management?

k) What is Business Continuity Plan?

l) What is Disaster Recover Plan?

m) What points to be considered during In-house Software Development?

n) What security mechanism should be undertaken by banks to secure its Internet Banking System?

0) What security mechanism should be undertaken by banks to secure its Credit Cards?

19. What is PCI-DSS? Why Banks should undertake PCI-DSS certification?
20. What is BS 7799? Write history of BS 7799.
21. What is ISO 27001? Write Why banks should acquire certification on ISO 27001 standard?
22. What are the 14 domains of ISO 27001?

23. What is a Cyber Law? Narrate any five of the Cyber Crime activities.
24. Describe ICT Act and mention applicable fields of ICT Act-2006.
25. Write Clause-56: Hacking with Computer System.

মডিউল-ই

# ডকুমেন্ট হ্যান্ডলিং পদ্ধতি, অতিরিক্ত ব্যাংকিং অ্যাপ্লিকেশন এবং অন্যান্য দিক

## ১. চেক প্রসেসিং সিস্টেম (Cheque Processing System)

চেক প্রসেসিং সিস্টেম বা সংক্ষেপে **পেমেন্ট সিস্টেম**, একটি মাধ্যম যার মাধ্যমে আর্থিক প্রতিষ্ঠান, ব্যবসা এবং ব্যক্তিদের মধ্যে তহবিল স্থানান্তর করা হয়। পেমেন্ট সিস্টেম একটি দেশের আর্থিক ব্যবস্থা ভালোভাবে কাজ করার জন্য এবং কেন্দ্রীয় ব্যাংক দ্বারা আর্থিক নীতিগুলোর সফল প্রয়োগের জন্য সবচেয়ে গুরুত্বপূর্ণ কারণ হিসাবে বিবেচনা করা হয়। অধিকন্তু পেমেন্ট পদ্ধতির আন্তঃসীমান্ত (cross border) সংযোগ একটি দেশের উন্নয়নের জন্য এবং বিদেশি পুঁজি ও বিদেশি বিনিয়োগকারীদের আকৃষ্ট করতে অপরিহার্য হয়ে ওঠে।

## ১.১. ক্লিয়ারিং ও সেটেলমেন্ট সিস্টেম (Clearing and Settlement Systems)

বর্তমানে বাংলাদেশে চারটি ক্লিয়ারিং পদ্ধতি চালু রয়েছে। সেগুলো হলো—

(ক) ঢাকায় বাংলাদেশ ব্যাংকের ক্লিয়ারিং হাউস এবং আরও সাতটি শহরে এর শাখা;

(খ) ৩১টি শহরে যেখানে বাংলাদেশ ব্যাংকের কোনো শাখা নেই সেখানে সোনালী ব্যাংকের ক্লিয়ারিং হাউস।

(গ) বাংলাদেশ ব্যাংকের বড় মূল্যের চেক সেটেলমেন্ট সিস্টেম; এবং

(ঘ) ঢাকায় বাংলাদেশ ব্যাংকের ফরেন কারেন্সি ক্লিয়ারিং সিস্টেম, যা ফরেক্স রিজার্ভ অ্যান্ড ট্রেজারি ম্যানেজমেন্ট ডিপার্টমেন্ট (FRTMD) দ্বারা বৈদেশিক মুদ্রার চেক ও পেমেন্ট ওর্ডার ক্লিয়ার ও সেটেলম্যান্ট করে।

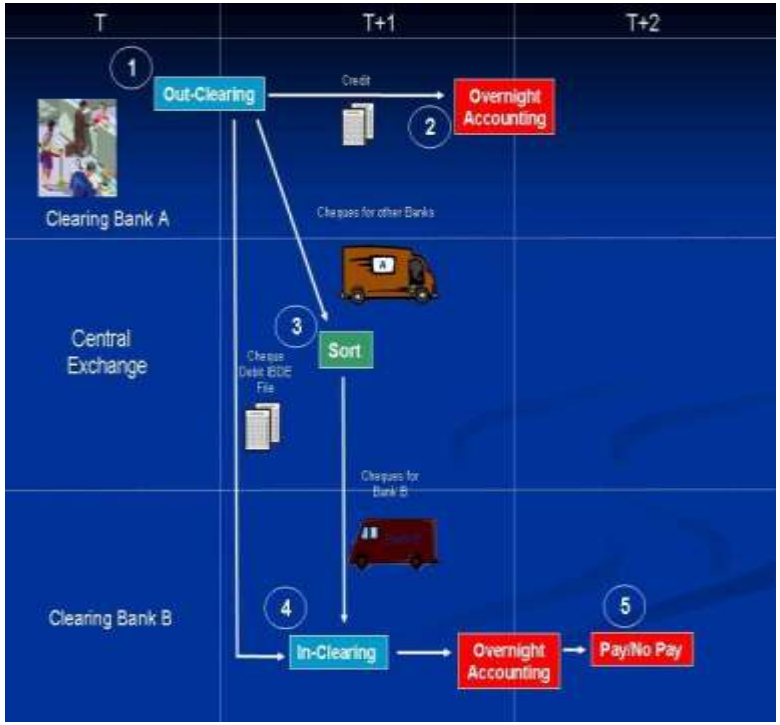
বাংলাদেশ ব্যাংকের ক্লিয়ারিং হাউসে প্রতিদিন চারটি ক্লিয়ারিং হয়। প্রথম ক্লিয়ারিং সকাল ১০:৩০ এ শুরু হয় এবং প্রথম ক্লিয়ারিং এর রিটার্ন হয় বিকাল ৫:৩০-এ। একই দিন (Same day) ক্লিয়ারিং শুরু হয় ১১:০০ এ এবং রিটার্ন হয় বিকাল ২:০০-এ। ক্লিয়ারিং হাউসের মাধ্যমে ক্লিয়ার করা উপকরণগুলো হলো চেক, ব্যাংক ড্রাফ্ট, পে-অর্ডার, ডিভিডেন্ড ওয়ারেন্ট, ইত্যাদি বরিশাল ও রংপুর অফিস ব্যতীত, বাংলাদেশ ব্যাংকের অন্যান্য শাখা অফিসে একটি কম্পিউটারাইজড

নিষ্পত্তি প্রক্রিয়া রয়েছে, যেখানে বাণিজ্যিক ব্যাংকগুলো, ফিজিক্যাল ইনস্ট্রুম্যান্ট ছাড়াও, ডিস্কেট পাঠায় যেখানে প্রতিটি ব্যাংকের পেমেন্ট অবলিগেশন ও অন্যান্য ব্যাংক থেকে পাওনার হিসাব থাকে। ঢাকা এবং চট্টগ্রামের তুলনায়, বাইরের শাখাগুলোতে ক্লিয়ার করা চেকের পরিমান খুবই কম।

## ১.২. প্রচলিত চেক ক্লিয়ারিং প্রক্রিয়া (Conventional Cheque Clearing Process)

প্রচলিত চেক ক্লিয়ারিং প্রসেস একটি মোটামুটি সময়সাপেক্ষ প্রক্রিয়া এবং এতে অনেক ম্যানুয়াল প্রক্রিয়া এবং ইনস্ট্রুম্যান্টের ফিজিক্যাল চলাচল জড়িত। এটি কেবল ক্লিয়ার করার সময়ই বৃদ্ধি করে না, বরং বিভিন্ন স্থানে ও বিভিন্ন ব্যক্তির মাধ্যমে ইনস্ট্রুমেন্ট চলাচলের কারণে উচ্চ স্তরের ঝুঁকি ও জালিয়াতির সম্ভাবনা দেখা দেয়।

এই ধরনের ক্লিয়ারিং প্রক্রিয়ার জীবন-প্রক্রিয়া নিম্নরূপ—

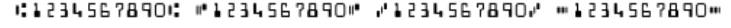



## ১.৩. MICR (ম্যাগনেটিক ইঙ্ক ক্যারেক্টার রিকগনিশন)

যেহেতু ম্যানুয়াল বা প্রচলিত চেক-ক্লিয়ারিং প্রক্রিয়া সময়সাপেক্ষ, তাই এমআইসিআর এর প্রবর্তন কার্যকর হয়েছে। ম্যাগনেটিক ইঙ্ক ক্যারেক্টার রিকগনিশন, বা এমআইসিআর হলো একটি ক্যারেক্টার রিকগনিশন প্রযুক্তি যা প্রাথমিকভাবে ব্যাংকিং শিল্প দ্বারা চেক প্রক্রিয়াকরণের সুবিধার্থে ব্যবহৃত হয়। প্রযুক্তিটির সাহায্যে কম্পিউটার চেক বা অন্যান্য আর্থিক লেনদেনের ডকুমেন্টের নিচে মুদ্রিত তথ্য (যেমন অ্যাকাউন্ট নম্বর, চেক নম্বর এবং বিশেষ অক্ষর) পড়তে পারে। বারকোড বা অনুরূপ প্রযুক্তির বিপরীতে, এমআইসিআর কোডগুলো মানুষ সহজেই পড়তে পারে।

এমআইসিআর অক্ষরগুলো চুম্বকীয় কালি বা টোনার যেখানে আয়রন অক্সাইড থাকে তা দিয়ে বিশেষ টাইপফেসে মুদ্রিত হয়। মেশিন এমআইসিআর লেখাকে ডিকোড করার সময়, এটি প্রথমে কাগজের সমতলে অক্ষরগুলোকে চুম্বকায়িত করে। তারপরে অক্ষরগুলো একটি এমআইসিআর রিড হেড, যা একটি টেপ রেকর্ডারের প্লেব্যাক হেডের মতো দেখতে, তার ওপর দিয়ে প্রেরণ করা হয়। প্রতিটি অক্ষর হেডের ওপর দিয়ে যাওয়ার সময় একটি অনন্য তরঙ্গ তৈরি করে, যা সিস্টেম দ্বারা সহজেই শনাক্ত করা যায়। এমআইসিআর প্রযুক্তি বাংলাদেশ সহ অনেক দেশের ব্যাংকিং শিল্পে ব্যবহৃত হয় কারণ এটি দ্রুত ও নির্ভরযোগ্য ডকোমেন্ট প্রক্রিয়া করতে সাহায্য করে।

বিশ্বজুড়ে ব্যবহৃত প্রধান এমআইসিআর ফন্ট হলো ই-১৩বি এবং সিএমসি-৭। ই-১৩বি অক্ষর ক্রমটি নিম্নরূপ—



যেখানে সিএমসি-৭ অক্ষর ক্রম নিম্নরূপ—

## ১.৪. চেক ট্রাঙ্কেশন (Cheque Truncation)

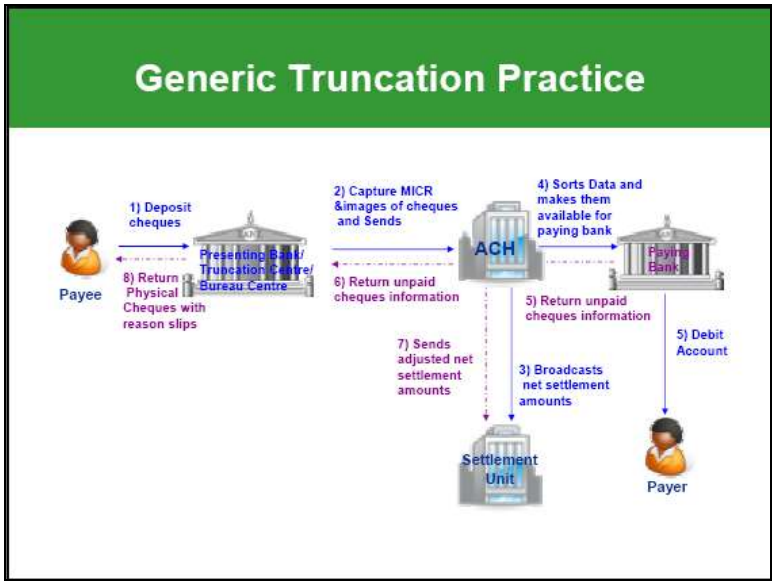
চেক ট্রাঙ্কেশন হলো ড্রয়ার (drawer) কর্তৃক ড্রয়ি (drawee) শাখার ওপর জারি করা কাগজের চেকের প্রবাহ বন্ধ করার প্রক্রিয়া। ফিজিক্যাল ইন্‌স্ট্রোম্যান্টটি গ্রহণকারী শাখায় যাওয়ার পথে এক পর্যায়ে ট্রাঙ্কেট করা হয় এবং চেকের একটি ইলেকট্রনিক ছবি ড্রয়ি শাখায় এমআইসিআর ফিল্ড, উপস্থাপনের তারিখ, উপস্থাপিত ব্যাংক, ইত্যাদির মতো প্রাসঙ্গিক তথ্যসহ পাঠানো হবে। চেক ট্রাঙ্কেশন বাস্তবায়নের ফলে, ব্যতিক্রমী পরিস্থিতিতে ছাড়া, শাখা/ব্যাংক জুড়ে ফিজিক্যাল ইনস্ট্রুম্যান্ট চলাচলের প্রয়োজন হয় না। এটি কার্যকরভাবে চেক পেমেন্টের জন্য

প্রয়োজনীয় সময়, ট্রানজিটের সংশ্লিষ্ট ব্যয় ও প্রক্রিয়াকরণে বিলম্ব ইত্যাদি কমিয়ে দেবে। ফলে এটি চেক সংগ্রহ বা আদায়ের প্রক্রিয়াকে ত্বরান্বিত করে।

চেক ট্রাঙ্কেশন সিস্টেম বা সিটিএস, চেক ক্লিয়ার করতে একটি নিরাপদ, সুরক্ষিত, দ্রুত ও কার্যকরী পদ্ধতি উপহার দেয়। সিটিএস-এ উপস্থাপক (Presenting) ব্যাংক তাদের 'ইমেজ ক্যাপচার সিস্টেম' ব্যবহার করে চেকের তথ্য ও ছবি নিজ দায়িত্বে সংগ্রহ করবে। তাদের ডেটা ও ছবির জন্য নির্ধারিত স্পেসিফিকেশন ও স্ট্যান্ডার্ড বজায় রাখবে। সুরক্ষা, নিরাপত্তা ও অপ্রত্যাখ্যান (non-repudiation) নিশ্চিত করতে PKI (পাবলিক কী ইনফ্রাস্ট্রাকচার) সিস্টেম জুড়ে প্রয়োগ করতে হবে। ব্যাংকগুলো সংগৃহীত ছবি এবং ডেটা পরবর্তীতে পেয়ি বা ড্রয়ি ব্যাংকে প্রেরণের উদ্দেশ্যে সেন্ট্রাল ক্লিয়ারিং হাউসে পাঠাবে।

উপরোক্ত উদ্দেশ্যের জন্য, বাংলাদেশ ব্যাংক সমস্ত ব্যাংককে Participating Bank Module বা পিবিএম নামে একটি সফ্টওয়্যার প্রদান করেছে যা তাদের ক্লিয়ারিং হাউস (CH) এর সঙ্গে একটি নিরাপদ উপায়ে এবং অ-প্রত্যাখ্যানসহ (non-repudiation) সংযোগ সৃষ্টি করে ডেটা প্রেরণ করতে সক্ষম করে। ক্লিয়ারিং হাউস ডেটা প্রসেস করে, ব্যাংকগুলোর সেটেলম্যান্ট এর পরিমাণ নির্ধারণ করে, এবং তাদের প্রান্তে প্রক্রিয়াকরণের জন্য পেয়ি বা ড্রয়ি ব্যাংকে প্রয়োজনীয় তথ্য প্রেরন করে। ড্রয়ি বা পেয়ি ব্যাংক ক্লিয়ারিং হাউস থেকে ডেটা ও ছবিগুলো পাওয়ার জন্য তাদের পিবিএম ব্যবহার করবে। ইনওয়ার্ড ডেটা ও ছবিগুলো প্রক্রিয়াকরণ করা ও পেমেন্ট করা যায়নি এমন ইনস্ট্রোম্যান্ট সমূহের জন্য রিটার্ন ফাইল তৈরি করার দায়িত্ব ড্রয়ি ব্যাংকের 'ইমেজ ক্যাপচার সিস্টেম' এর উপর ন্যাস্ত।

সাধারণ ট্রাঙ্কেশন অনুশীলনগুলো নিম্নরূপ—




ব্যাংকের পক্ষ থেকে সিটিএস-এর জন্য প্রয়োজনীয় পরিকাঠামো হলো, সিটিএস অ্যাপ্লিকেশনের জন্য ব্যাংক গেটওয়ে থেকে ক্লিয়ারিং হাউস, হার্ডওয়্যার ও সফ্টওয়্যার পর্যন্ত সংযোগ স্থাপন করা। বাংলাদেশ ব্যাংক সদস্য ব্যাংকগুলোকে PBM সরবরাহ করবে এবং ব্যাংকগুলোকে CH-এর জন্য অন্যান্য হার্ডওয়্যার ও সিস্টেম সফ্টওয়্যার এবং তাদের ক্যাপচার সিস্টেমের জন্য প্রয়োজনীয় অ্যাপ্লিকেশন সফ্টওয়্যার তাদের নিজস্বভাবে সংগ্রহ করতে হবে।

এই ধরনের পদ্ধতির কিছু সুবিধা হলো—

- দ্রুত ক্লিয়ারিং চক্র।
- উন্নত রিকনসিলিয়েশন/যাচাই প্রক্রিয়া।
- উন্নত গ্রাহক পরিষেবা, উন্নত গ্রাহক উইন্ডো।
- T+0 বা T+1 ক্লিয়ারিং দিন।
- ফ্লোট এর প্রয়োজনীয়তা নেই। ক্রেডিট পুশ পেমেন্টে স্থানান্তরিত করতে প্রণোদনা।
- ক্লিয়ারিং হাউসের এখতিয়ার সমগ্র দেশে প্রসারিত করা সম্ভব। ভৌগোলিক নির্ভরতা নেই।
- অপারেশনাল দক্ষতা ব্যাংকগুলোর অধস্তনদেরকে উপকৃত করবে।
- লেনদেনের খরচ কমে যায়।
- ট্রান্সমিশন রুট সুরক্ষিত করে পরিচালনার ঝুঁকি কমায়।

### ১.৫. RTGS (রিয়েল টাইম গ্রস সেটেলমেন্ট)

রিয়েল টাইম গ্রস সেটেলমেন্ট (RTGS) পদ্ধতি হলো ফান্ড ট্রান্সফার সিস্টেম যেখানে অর্থ বা সিকিউরিটিগুলো 'রিয়েল-টাইম' ও 'গ্রস' ভিত্তিতে এক ব্যাংক থেকে অন্য ব্যাংকে স্থানান্তর করা হয়। এটি ব্যাংকিং চ্যানেলের মাধ্যমে দ্রুততম সম্ভাব্য অর্থ স্থানান্তর ব্যবস্থা। 'রিয়েল টাইমে' নিষ্পত্তি মানে অর্থপ্রদানের লেনদেনে কোনো ওয়েটিং টাইম নেই।

লেনদেনগুলো প্রক্রিয়া হওয়ার সঙ্গে সঙ্গে নিষ্পত্তি করা হয়। 'গ্রস সেটেলমেন্ট' মানে অন্য কোনো লেনদেনের সাথে গুচ্ছ বা নেটিং না করে এক থেকে এক ভিত্তিতে লেনদেন নিষ্পত্তি করা হয়। কেন্দ্রীয় ব্যাংকের বইয়ে অর্থ স্থানান্তর সংঘটিত হয় তা বিবেচনা করে, অর্থ প্রদানকে চূড়ান্ত ও অপরিবর্তনীয় হিসাবে বিবেচনা করা হয়।

### ১.৬. BACH (বাংলাদেশ অটোমেটেড ক্লিয়ারিং হাউস)

বাংলাদেশ ব্যাংক 'বাংলাদেশ অটোমেটেড ক্লিয়ারিং হাউস' (BACH) নামে দেশের পেমেন্ট সিস্টেম স্বয়ংক্রিয়করণের প্রকল্প বাস্তবায়ন করেছে। প্রকল্পটি দুটি অংশে বিভক্ত—

i) BACPS (বাংলাদেশ অটোমেটেড চেক প্রসেসিং সিস্টেম) এবং
ii) BEFTN (বাংলাদেশ ইলেকট্রনিক ফান্ড ট্রান্সফার নেটওয়ার্ক)।

#### ১.৬.১. বাংলাদেশ অটোমেটেড চেক প্রসেসিং সিস্টেম (BACPS)

বাংলাদেশ ব্যাংক ২০১০ সালে বিএসিপিএস চালু করেছে। বিএসিপিএস চেক ইমেজিং এবং ট্রাঙ্কেশন কার্যক্রমের সঙ্গে বাস্তবায়িত হয়েছে।

তদনুসারে, ব্যাংকগুলোর জন্য চেকের নকশা উন্নত করা হয়েছে। আকার, নিরাপত্তা বৈশিষ্ট্য ও কাগজের স্পেসিফিকেশন আর্থিক প্রতিষ্ঠানগুলোকে জানানো হয়েছে। নতুন চেকের পাতায় একটি ম্যাগনেটিক ইঙ্ক ক্যারেক্টার রিকগনিশন (MICR) রেখা রয়েছে যা পরিমান, ট্রেনজেকশন কোড, গ্রাহকদের অ্যাকাউন্টের তথ্য, রাউটিং নম্বর এবং চেক লিফের সিরিয়াল নম্বর ধারনের জন্য ডিজাইন করা হয়েছে।

চেকের উৎপত্তি এবং গন্তব্য সহজে শনাক্ত করার জন্য নতুন রাউটিং নম্বর ব্যাংক শাখাতে বণ্টন করা হয়েছে। রাউটিং নম্বরটি ৯টি সংখ্যা নিয়ে গঠিত। প্রথম ৩ সংখ্যা হলো ব্যাংক কোড, পরের ২ সংখ্যা হলো জেলা কোড, পরবর্তী ৩ সংখ্যা হলো শাখা কোড এবং শেষ সংখ্যা হলো চেক ডিজিট।

সিস্টেমটি ইন্ট্রা-রিজিওনাল ও ইন্টার-রিজিওনাল ক্লিয়ারিং উভয়কেই সমর্থন করবে। সিস্টেমটি ঢাকায় অবস্থিত একটি সেন্ট্রালাইজড প্রসেসিং সেন্টার এবং ৬৪টি জেলায় এর সার্ভিস শাখাগুলোর ওপর ভিত্তি করে তৈরি করা হয়। প্রস্তাবিত প্রক্রিয়া ও পদ্ধতিগুলো সর্বোত্তম অনুশীলনের (best practice) সঙ্গে সামঞ্জস্যপূর্ণ এবং এটি চেক প্রক্রিয়াকরণের জন্য সবচেয়ে সাশ্রয়ী সমাধান। বিএসিপিএস প্রকল্পের প্রথম ধাপ, অর্থাৎ ঢাকা ক্লিয়ারিং হাউস ৭ অক্টোবর, ২০১০ থেকে চালু রয়েছে।

#### ১.৬.২. বাংলাদেশ ইলেকট্রনিক ফান্ড ট্রান্সফার নেটওয়ার্ক (BEFTN)

বিইএফটিএন সমস্ত অংশগ্রহণকারী ব্যাংকের মধ্যে ইলেকট্রনিক ডেবিট ও ক্রেডিট ইনস্ট্রুমেন্টের বিতরণ ও নিষ্পত্তির জন্য একটি প্রক্রিয়াকরণ ও বিতরণ কেন্দ্র হিসাবে কাজ করবে। বিইএফটিএন নেটওয়ার্ককে যোগাযোগ লাইনের মাধ্যমে ইএফটি অপারেটরের সঙ্গে সংযুক্ত পার্টিসিপেটিং ব্যাংকগুলোর একটি পদ্ধতি হিসাবে কল্পনা করা যায়। এই নেটওয়ার্কটি ইলেকট্রনিকভাবে ব্যাংকগুলোর মধ্যে অর্থ হস্তান্তরকে সহজতর করে, যা বিদ্যমান কাগজভিত্তিক পদ্ধতির তুলনায় আন্তঃব্যাংক ক্লিয়ারিংয়ের দ্রুত এবং আরও কার্যকর উপায় তৈরি করেছে।

নেটওয়ার্কটি সহজ ক্রেডিট লেনদেন দিয়ে শুরু হয় এবং ধীরে ধীরে ডেবিট লেনদেনে অগ্রসর হয়েছে। এটি নাটকীয়ভাবে অপারেশনাল খরচ কমিয়ে আনে, ঝুঁকি কমিয়ে দেয় এবং পেমেন্ট প্রক্রিয়ার দক্ষতাও বাড়ায়।

BEFTN, ইলেকট্রনিক ফান্ড ট্রান্সফারের একটি উপায়, ডিফার্ড নেট সেটেলমেন্ট (ডিএনএস) ভিত্তিতে কাজ করে যা ব্যাচে লেনদেন নিষ্পত্তি করে। ডিএনএস-এ, একটি নির্দিষ্ট সময়ে নিষ্পত্তি সংঘটিত হয়। সমস্ত লেনদেন সেই সময় পর্যন্ত আটকে থাকে। উদাহরণস্বরূপ, যদি ইএফটি নিষ্পত্তি সপ্তাহের অফিস দিনগুলোতে দিনে ২ বার হয় (উদাহরণস্বরূপ সকাল ১১:০০ এবং বিকাল ৩:০০ এ), তখন নির্ধারিত নিষ্পত্তির সময়ের পরে শুরু হওয়া যেকোনো লেনদেন পরবর্তী নির্ধারিত নিষ্পত্তির সময় পর্যন্ত অপেক্ষা করবে। অন্যদিকে, আরটিজিএস-এ, লেনদেনগুলো ক্রমাগতভাবে আরটিজিএস চালুকালীন সময়ে প্রক্রিয়া করা হয়।

## ২. অতিরিক্ত ব্যাংকিং অ্যাপ্লিকেশন (Additional Banking Application)

### ২.১. ইআরপি সফটওয়্যার (ERP Software)

#### ২.১.১. ইআরপি সিস্টেম কী?

ইআরপি (এন্টারপ্রাইজ রিসোর্স প্ল্যানিং) হলো একটি সমন্বিত কম্পিউটারভিত্তিক পদ্ধতি যা অভ্যন্তরীণ এবং বাহ্যিক রিসোর্সসমূহ পরিচালনা করতে ব্যবহৃত হয়, যার মধ্যে টেনজিবল অ্যাসেট, আর্থিক রিসোর্স, উপকরণ ও মানব সম্পদ রয়েছে। এর উদ্দেশ্য হলো সংস্থার সীমানার মধ্যে সমস্ত ব্যবসায়িক কার্যক্রমের মধ্যে তথ্যের প্রবাহকে সহজতর করা এবং বাইরের অংশীদারদের সঙ্গে সংযোগগুলো ম্যানেজ করা। একটি কেন্দ্রীভূত ডাটাবেসের ওপর নির্মিত এবং একটি কমন কম্পিউটিং প্ল্যাটফর্ম ব্যবহার করে, ইআরপি সিস্টেম সমস্ত ব্যবসায়িক ক্রিয়াকলাপকে একটি অভিন্ন ও প্রতিষ্ঠানভিত্তিক সিস্টেমে একীভূত করে।

একটি ইআরপি পদ্ধতি হয় একটি কেন্দ্রীভূত সার্ভারে থাকে বা হার্ডওয়্যার এবং সফ্টওয়্যারে মডিউলার আকারে বিস্তৃত থাকে, যা 'পরিষেবা' প্রদান করে এবং লোকাল এরিয়া নেটওয়ার্ক (LAN) এর মাধ্যমে যোগাযোগ করে। ডিস্ট্রিবিউটেড্ ডিজাইন একটি ব্যবসাকে বিভিন্ন বিক্রেতাদের কাছ থেকে মডিউল একত্রিত করার সুবিধা দেয়, ফলে জটিল ও ব্যয়বহুল কম্পিউটার সিস্টেমের একাধিক কপি স্থাপনের প্রয়োজন নেই।

একটি সফ্টওয়্যারকে ইআরপি সিস্টেম হিসাবে বিবেচনা করার জন্য, নিম্নলিখিত বৈশিষ্ট্যগুলো থাকা উচিত :

—ইন্ট্রিগেটেড হতে হবে এবং কোনো পিরিয়ডিক ব্যাচ হালনাগাদ ছাড়াই রিয়েল-টাইমে কাজ করতে হবে।

—রিডান্ডেন্ট ডেটা ও একাধিক ডেটা ডেফিনেশন প্রতিরোধ করতে সকল অ্যাপ্লিকেশনের জন্য একটি ডাটাবেস থাকবে।

—সমস্ত মডিউলের একই লুক এন্ড ফিল (look&feel) থাকবে।

—ব্যবহারকারীরা IS বিভাগের সাহায্য ছাড়াই সিস্টেমের যেকোনো ডেটা অ্যাক্সেস করতে পারবে।

### ২.১.২. একটি ইআরপি সফ্টওয়্যারের কম্পোনেন্ট/ মডিউল

ক) লেনদেনের ভিত্তি (Transactional Backbone)

- আর্থিক
- ডিস্ট্রিবিউশন
- মানব সম্পদ
- পণ্য লাইফ সাইকেল ব্যবস্থাপনা

খ) উন্নত অ্যাপ্লিকেশন (Advanced Applications)

- কাস্টমার রিলেশনশিপ ম্যানেজমেন্ট (CRM)
- সাপ্লাই চেইন ম্যানেজমেন্ট সফটওয়্যার
  - পার্সেজিং
  - ম্যানুফেকচারিং
  - ডিস্ট্রিবিউশন
  - ওয়্যারহাউজ ব্যবস্থাপনা পদ্ধতি

গ) ম্যানেজম্যান্ট পোর্টাল/ড্যাশবোর্ড (Management Portal/ Dashboard)
—ডিসিশন সাপোর্ট পদ্ধতি

একটি ব্যাংকে, নিম্নলিখিত মডিউলগুলো উপযুক্ত হতে পারে

ক) মানব সম্পদ ব্যবস্থাপনা (এইচআরএম)

খ) কাস্টমার রিলেশনশিপ ম্যানেজমেন্ট (CRM)

গ) সাপ্লাই-চেইন ম্যানেজমেন্ট

- পার্সেজিং
- ডিস্ট্রিবিউশন

ঘ) ওয়্যারহাউজ ব্যবস্থাপনা (অ্যাসেট ব্যবস্থাপনা)

### ২.১.৩. একটি ইআরপি সিস্টেমের কম্পোনেন্ট

ক) ম্যানুফেকচারিং

প্রকৌশল, উপাদানের বিল, কাজের আদেশ, সময়সূচি, ক্ষমতা, কর্মপ্রবাহ ব্যবস্থাপনা, মান নিয়ন্ত্রণ, খরচ ব্যবস্থাপনা, উৎপাদন প্রক্রিয়া, উৎপাদন প্রকল্প, এবং উৎপাদন প্রবাহ।

খ) সরবরাহ চেইন ব্যবস্থাপনা :

নগদ অর্ডার, ইনভেন্টরি, অর্ডার এন্ট্রি, ক্রয়, পণ্য কনফিগারার, সাপ্লাই চেইন পরিকল্পনা, সরবরাহকারীর সময়সূচি, পণ্য পরিদর্শন, দাবি প্রক্রিয়াকরণ ও কমিশন হিসাব।

গ) ফাইন্যান্সিয়েল :

জেনারেল লেজার, নগদ ব্যবস্থাপনা, প্রদেয় হিসাব, প্রাপ্য হিসাব, স্থায়ী সম্পদ।

ঘ) প্রকল্প ব্যবস্থাপনা :

খরচ, বিলিং, সময় এবং ব্যয়, কর্মক্ষমতা ইউনিট, কার্যকলাপ ব্যবস্থাপনা।

ঙ) মানব সম্পদ :
মানব সম্পদ, পে-রোল, প্রশিক্ষণ, সময় এবং এটেন্ডেন্স, রোস্টারিং, বেনিফিটস্।

চ) গ্রাহক সম্পর্ক ব্যবস্থাপনা (Customer Relationship Management):
বিক্রয় ও বিপণন, কমিশন, পরিষেবা, গ্রাহক যোগাযোগ, কল-সেন্টার সাপোর্ট।

ছ) ডেটা পরিষেবা :
গ্রাহক, সরবরাহকারী এবং/অথবা কর্মচারীদের জন্য বিভিন্ন Self-service ইন্টারফেস।

জ) অ্যাক্সেস নিয়ন্ত্রণ
বিভিন্ন প্রক্রিয়ার জন্য ব্যবহারকারীর বিশেষাধিকার ব্যবস্থাপনা।

### ২.১.৪. ইআরপি সিস্টেমের সুবিধা ও অসুবিধা

সুবিধাদি—

—বিশ্বব্যাপী ইন্ট্রিগেশন সহজ হয় (মুদ্রা বিনিময় হার, ভাষা ও সংস্কৃতির বাধা স্বয়ংক্রিয়ভাবে দূর করা যায়)।

—কোম্পানি ব্যাপি আপডেট প্রয়োগের জন্য শুধু একবার আপডেট করতে হয়।

—রিডান্ডেন্সি ত্রুটি কমিয়ে রিয়েল-টাইম তথ্য সরবরাহ করে।

—কর্মীদের জন্য আরও দক্ষ কাজের পরিবেশ তৈরি করে।

—কীভাবে সর্বোত্তমভাবে একটি পদ্ধতি তৈরি এবং বাস্তবায়ন করা যায় সে ব্যাপারে ভেন্ডরদের অতীত জ্ঞান ও দক্ষতা রয়েছে।

অসুবিধা :

—ভেন্ডরের সঙ্গে চুক্তি ও ম্যানেজিবিলিটির মাধ্যমে সম্পর্কের লক করা। একটি চুক্তি মেয়াদ শেষ না হওয়া পর্যন্ত একটি কোম্পানিকে ভেন্ডরের কাছে ধরে রাখতে পারে এবং যদি সুইচিং খরচ খুব বেশি হয় তবে ভেন্ডর পরিবর্তন করা অলাভজনক হতে পারে।

—অনমনীয়তা—ভেন্ডরের প্যাকেজগুলো একটি কোম্পানির ব্যবসায়িক মডেলের সঙ্গে সঠিকভাবে উপযুক্ত নাও হতে পারে এবং কাস্টমাইজেশন ব্যয়বহুল হতে পারে।

—বিনিয়োগে রিটার্ন লাভজনক হতে খুব বেশি সময় লাগতে পারে।

—বাস্তবায়নে প্রকল্পের ব্যর্থতার ঝুঁকি থাকে।

### ২.১.৫. বিখ্যাত ইআরপি সফটওয়্যারসমূহ

#### ২.১.৫.১. এসএপি এর এসএপি ইআরপি (SAP ERP from SAP)

এসএপি (সিস্টেম অ্যানালাইসিস অ্যান্ড প্রোগ্রাম ডেভেলপমেন্ট) হলো একটি জার্মান সফ্টওয়্যার কর্পোরেশন যেটি এন্টারপ্রাইজ সফ্টওয়্যার অ্যাপ্লিকেশন এবং বিশ্বব্যাপী সমস্ত আকারের ব্যবসায়িক সহায়তা প্রদান করে। জার্মানির ওয়ালডর্ফ-এ সদর দপ্তর, সারা বিশ্বে আঞ্চলিক অফিসসহ, এসএপি হলো বিশ্বের বৃহত্তম এন্টারপ্রাইজ সফ্টওয়্যার কোম্পানি (২০০৯ অনুযায়ী)। এটি ইউরোপের বৃহত্তম সফ্টওয়্যার কোম্পানি এবং বিশ্বে চতুর্থ বৃহত্তম। কোম্পানির সবচেয়ে পরিচিত পণ্য হলো এর এসএপি এন্টারপ্রাইজ রিসোর্স প্ল্যানিং (এসএপি ইআরপি) ও এসএপি বিজনেস অবজেক্টস সফটওয়্যার।

এসএপি ইআরপি অ্যাপ্লিকেশন হলো এসএপি এজি দ্বারা নির্মিত একটি সমন্বিত এন্টারপ্রাইজ রিসোর্স প্ল্যানিং (ইআরপি) সফ্টওয়্যার যা সমস্ত শিল্প ও সেক্টরে মাঝারি আকারের এবং বড় প্রতিষ্ঠানের ব্যবসায়িক সফ্টওয়্যার প্রয়োজনীয়তাকে লক্ষ্য করে তৈরি করা হয়েছে। এটি কোম্পানির সমস্ত কার্যক্রমের মধ্যে এবং কোম্পানিগুলোর মধ্যে ওপেন কমিউনিকেশনের সুযোগ সৃষ্টি করে।

এসএপি এর ইআরপি সমাধানে বেশ কয়েকটি মডিউল রয়েছে, যা মূল কার্যকরী ক্ষেত্রগুলোকে সমর্থন করে, যার মধ্যে রয়েছে—

—এসএপি ইআরপি ফিন্যান্সিয়ালস

—এসএপি ইআরপি অপারেশন

—এসএপি ইআরপি হিউম্যান ক্যাপিটাল ম্যানেজমেন্ট

#### ২.১.৫.২. ওরাকলের পিপলসসফট ইআরপি (People Soft ERP froOracle)

ওরাকল কর্পোরেশন হলো একটি আমেরিকান বহুজাতিক কম্পিউটার প্রযুক্তি কর্পোরেশন যা এন্টারপ্রাইজ সফ্টওয়্যার পণ্য—বিশেষত ডাটাবেস ম্যানেজমেন্ট সিস্টেমের তৈরি ও বিপণনে বিশেষজ্ঞ। রেডউড শোরস, ক্যালিফোর্নিয়া, মার্কিন যুক্তরাষ্ট্রে সদর দপ্তর অবস্থিত, ওরাকল ১ জুলাই ২০১০ পর্যন্ত বিশ্বব্যাপী ১০৫,০০০

লোককে নিয়োগ দেয়। এটি অরগানিক বৃদ্ধির মাধ্যমে এবং বেশ কয়েকটি উচ্চ-মানের প্রযুক্তি অধিগ্রহণের মাধ্যমে সফ্টওয়্যার বাজারে এর প্রাধান্যকে বাড়িয়েছে। মাইক্রোসফ্ট ও আইবিএম-এর পরে ২০০৭ সালের মধ্যে ওরাকলের আয়ের দিক থেকে তৃতীয় বৃহত্তম সফ্টওয়্যার কোম্পানি।

কর্পোরেশনটি তার শীর্ষস্থানীয় পণ্য, ওরাকল ডেটাবেসের জন্য সর্বাধিক পরিচিত হয়ে উঠেছে। কোম্পানিটি ডাটাবেস উন্নয়ন এবং মধ্য-স্তরের (Middle-tier) সফ্টওয়্যার, এন্টারপ্রাইজ রিসোর্স প্ল্যানিং সফ্টওয়্যার (ইআরপি), গ্রাহক সম্পর্ক ব্যবস্থাপনা সফ্টওয়্যার (সিআরএম) এবং সরবরাহ চেইন ব্যবস্থাপনা (এসসিএম) সফ্টওয়্যার পদ্ধতি তৈরি করে।

২০১০ সাল পর্যন্ত ওরাকল কর্পোরেশনের সহ-প্রতিষ্ঠাতা ল্যারি এলিসনসারা ওরাকলের প্রধান নির্বাহী কর্মকর্তা হিসেবে দায়িত্ব পালন করেন। এলিসন ২০০৪ সালে জেফরি ও. হেনলির স্থলাভিষিক্ত হওয়া পর্যন্ত বোর্ডের চেয়ারম্যান হিসেবেও দায়িত্ব পালন করেন। এলিসন প্রধান নির্বাহী কর্মকর্তা হিসেবে তার ভূমিকা বজায় রাখেন। ২২শে আগস্ট, ২০০৮-এ সহযোগী প্রেস প্রতিষ্ঠাতা ল্যারি এলিসনকে বিশ্বের শীর্ষ-পারিশ্রমিক পাওয়া প্রধান নির্বাহী হিসাবে গণ্য করা হয়।

পিপলসফ্ট, ইনকর্পোরেটেড এমন একটি কোম্পানি যা মানব সম্পদ ব্যবস্থাপনা পদ্ধতি (এইঅঅরএমএস) এবং গ্রাহক সম্পর্ক ব্যবস্থাপনা (সিআরএম) সফ্টওয়্যার, সেইসঙ্গে উৎপাদন, আর্থিক, এন্টারপ্রাইজ কর্মক্ষমতা ব্যবস্থাপনা এবং ছাত্র প্রশাসনের জন্য সফ্টওয়্যারগুলো বড় বড় কর্পোরেশন, সরকারি অফিস ও সংস্থাগুলোকে সরবরাহ করেছিল। ২০০৫ সালে ওরাকল কর্পোরেশন কর্তৃক অধিগ্রহণ না হওয়া পর্যন্ত এটি একটি স্বাধীন কর্পোরেশন হিসাবে বিদ্যমান ছিল। পিপলসফ্ট-এর পণ্য এখন ওরাকল দ্বারা বাজারজাত করা হয়।

**পিপলসফটের ইতিহাস**

—১৯৮৭ : ডেভিড ডাফিল্ড এবং কেন মরিস আমেরিকার ওয়ালনাট ক্রিক, সিএ, নামক জায়গায় পিপলসফট কর্পোরেশন প্রতিষ্ঠিত করেন।
—১৯৮৮ : পিপলসসফট HRMS প্রকাশিত হয়েছে।
—১৯৯৪ : ডিস্ট্রিবিউশন ও আর্থিক মডিউলের পাবলিক বিতরণ।
—১৯৯৫ : ছাত্র প্রশাসন ব্যবস্থার সূচনা।
—১৯৯৬ : ম্যানুফেকচারিং এর সূচনা।
—১৯৯৬ : পিপলসসফট ৬ প্রকাশ করে, যা তাদের প্রথম ইআরপি প্যাকেজ।
—২০০৫ : ওরাকল কর্পোরেশন দ্বারা অধিগ্রহণ।
—২০০৯ : পিপলসফট HCM 9.1 প্রকাশিত হয়। (অক্টোবর ২০০৯)
—২০০৯ : পিপলসফট FCM 9.1 প্রকাশিত হয়েছে। (নভেম্বর ২০০৯)

## ২.২. সিআরএম সফটওয়্যার (CRM Software)

### ২.২.১. সিআরএম কী?

সিআরএম (গ্রাহক সম্পর্ক ব্যবস্থাপনা) ক্রেতা, গ্রাহক ও বিক্রয়ের সঙ্গে জড়িত একটি কোম্পানির সমন্বিত পরিচালনা বাস্তবায়ন করার কৌশল। এটি ব্যবসায়িক প্রক্রিয়াগুলো যেমন প্রধানত বিক্রয় কার্যক্রম, সেগুলোর বিপণন, কাস্টমার সার্ভিস ও প্রযুক্তিগত সহায়তা ইত্যাদি স্বয়ংক্রিয়ভাবে সংগঠিত করতে এবং সিঙ্ক্রোনাইজ করতে প্রযুক্তি ব্যবহার করে।

সামগ্রিক লক্ষ্য হলো নতুন গ্রাহকদের খুঁজে বের করা, আকৃষ্ট করা এবং তাদের জয় করা, তাদের যত্ন নেওয়া এবং ধরে রাখা, পূর্বের গ্রাহকদের আবার ফিরিয়ে আনা এবং মার্কেটিং ও গ্রাহক পরিষেবার খরচ কমানো। গ্রাহক সম্পর্ক ব্যবস্থাপনা, গ্রাহক-ইন্টারফেস বিভাগ এবং অন্যান্য বিভাগসহ একটি কোম্পানির ব্যবসায়িক কৌশল বর্ণনা করে।

যে তিনটি ধাপে সিআরএম একটি ব্যবসা এবং এর গ্রাহকদের মধ্যে সম্পর্ককে সমর্থন করে তা হলো—

- অধিগ্রহণ করা: সিআরএম যোগাযোগ ব্যবস্থাপনা, বিক্রয় ও fullfillment-এর মাধ্যমে একটি সংস্থাকে নতুন নতুন গ্রাহক সংগ্রহে সহায়তা করতে পারে।
- উন্নত করা : গ্রাহক পরিষেবা টুলস-এর সঙ্গে একত্রিত ওয়েব-সক্ষম সিআরএম ব্যবহার করে বিক্রয় এবং পরিষেবা বিশেষজ্ঞদের দ্বারা গ্রাহকদের পরিষেবা প্রদান করে, যা গ্রাহকদের ওয়ান-স্টপ সুবিধা প্রদান করে।
- ধরে রাখা : সিআরএম সফ্টওয়্যার ও ডাটাবেস একটি সংস্থাকে এর অনুগত গ্রাহকদের শনাক্ত ও পুরস্কৃত করতে সাহায্য করে এবং মার্কেটিং ও মার্কেটিং-এর সঙ্গে সম্পর্কিত উদ্যোগকে আরও উন্নত করতে সাহায্য করে।

### ২.২.২. ব্যবহারের ক্ষেত্রসমূহ (Fields of Application)

#### ২.২.২.১. সেলস ফোর্স অটোমেশন (Sales force automation)

সেলস ফোর্স অটোমেশন (এসএফএ) বিক্রয় প্রক্রিয়ার সমস্ত পর্যায়কে সুসংহত করতে সফ্টওয়্যার ব্যবহার করে এবং প্রতিটি পর্যায়ে বিক্রয় প্রতিনিধিদের যে সময় ব্যয় করতে হবে তা হ্রাস করে। এটি বিক্রয় প্রতিনিধিদের অল্প সময়ের মধ্যে আরও বেশি গ্রাহকদের অনুপ্রাণিত করার সুযোগ দেয়। SFA-এর কেন্দ্রস্থলে হলো একটি কন্টাক্ট ব্যবস্থাপনা পদ্ধতি, যা প্রতিটি সম্ভাব্য গ্রাহকের জন্য প্রাথমিক কন্টাক্ট থেকে শেষ পর্যন্ত বিক্রয় প্রক্রিয়ার প্রতিটি পর্যায়ে অনুসরণ ও নথিবদ্ধ করতে সাহায্য করে। অনেক এসএফএ অ্যাপ্লিকেশনের মধ্যে opportunities, territories, বিক্রয়

পূর্বাভাস এবং ওয়ার্কফ্লো অটোমেশন, Quote তৈরি ও পণ্য সম্পর্কিত ব্যবহারিক জ্ঞান অন্তর্ভুক্ত থাকে। ওয়েব ২.০ ই-কমার্স ও প্রাইচিং মডিউলগুলো হচ্ছে এসএফএ-তে নতুন কিন্তু বিপুল আগ্রহ সৃষ্টি করেছে।

### ২.২.২.২. মার্কেটিং (Marketing)

বিপণনের জন্য সিআরএম পদ্ধতিগুলো এন্টারপ্রাইজকে তাদের সম্ভাব্য গ্রাহকদের চিহ্নিত ও টার্গেট করতে এবং বিক্রয় দলের জন্য লিড তৈরি করতে সহায়তা করে। একটি মূল বিপণন দক্ষতা হলো ইমেল, সার্চ, সোশ্যাল মিডিয়া, টেলিফোন ও সরাসরি মেইলসহ বহুমাত্রিক প্রচারাভিযানের ট্রাকিং ও পরিমাপ করা। নিরীক্ষণ করা মেট্রিক্স-এর মধ্যে ক্লিক করা, প্রতিক্রিয়া, লিড তৈরি, ডিল্স ও রেভিনিউ অন্তর্ভুক্ত। এটি 'বিপণনের স্বয়ংক্রিয়তা' এবং 'গ্রাহক সম্পর্ক ব্যবস্থাপনা' (পিআরএম) কর্তৃক স্থানান্তর করা হয়েছে, যা গ্রাহকদের আচরণকে অনুসরণ করে এবং প্রথম যোগাযোগ থেকে বিক্রয় পর্যন্ত তাদের পরিষেবা প্রদান করে।

### ২.২.২.৩. গ্রাহক সেবা ও সাপোর্ট (Customer Service and Support)

গ্রাহকদের আকৃষ্ট ও ধরে রাখার ক্ষেত্রে সেবা একটি গুরুত্বপূর্ণ বিষয়—এটি মাথায় রেখে সংস্থাগুলো দক্ষতা বৃদ্ধি ও খরচ কমানোর লক্ষ্যে তাদের গ্রাহকদের অভিজ্ঞতা উন্নত করতে প্রযুক্তির দিকে ঝুঁকছে। এ সত্ত্বেও, ২০০৯ সালের একটি সমীক্ষায় দেখা যায় যে শুধু ৩৯% কর্পোরেট নির্বাহী বিশ্বাস করেন যে গ্রাহক সমস্যা সমাধান করতে তাদের কর্মচারীদের সঠিক টুলস্ ও কর্তৃত্ব রয়েছে। উন্নত প্রযুক্তির কল রাউটিং, কম্পিউটার টেলিফোন ইন্টিগ্রেশন (সিটিএ) এবং তীব্র কর্মক্ষমতা সম্পন্ন বৈশিষ্ট্যগুলোসহ কল সেন্টার সল্যুশন আজও ঐ সব অ্যাপ্লিকেশনের মধ্যমণি হয়ে আছে।

### ২.২.২.৪ বিশ্লেষণ (Analysis)

প্রাসঙ্গিক বিশ্লেষণ সক্ষমতা প্রায় প্রতিটি বিক্রয়, বিপণন ও পরিষেবায় অ্যাপ্লিকেশনগুলোর মধ্যে থাকে। এই বৈশিষ্ট্যগুলো বিশ্লেষণ ও ব্যবসায়িক বুদ্ধিমত্তার জন্য তৈরি পৃথক, উদ্দেশ্য-নির্মিত অ্যাপ্লিকেশনগুলোর সাথে পরিপূরক ও পরিবর্ধিত হতে পারে। বিক্রয় বিশ্লেষণ (Sales analysis) কোম্পানিগুলোকে বিক্রয় পূর্বাভাস ও ডেটা কোয়ালিটির মাধ্যমে গ্রাহকের ক্রিয়াকলাপ ও পছন্দগুলো নিরীক্ষণ ও বুঝতে সাহায্য করে।

বিভাজন (segmentation) ও লক্ষ্য (targeting) উন্নত করতে ভবিষ্যদ্বাণীমূলক বিশ্লেষণ (Predictive analysis) এবং অনলাইন, অফলাইন ও অনুসন্ধান বিপণন প্রচারাভিযানের (search marketing campaign) কার্যকারিতা পরিমাপের জন্য বৈশিষ্ট্যগুলো বিপণন অ্যাপ্লিকেশনে থাকে। ওয়েব সাইটগুলো শুধু মাউস ক্লিক ট্র্যাক করা থেকে শুরু করে এ পর্যন্ত উল্লেখযোগ্যভাবে বিবর্তিত হয়েছে। 'বিক্রয় সিগন্যাল' মূল্যায়ন করে বিপণনকারীরা (marketers) দেখতে পারে যে কোনো লেনদেনগুলোর সম্ভাবনা সবচেয়ে বেশি এবং শনাক্ত করতে পারে কারা বিক্রয় প্রক্রিয়ার মধ্যে bogged down হয়ে পড়েছে, ফলে তাদের সহায়তার প্রয়োজন। Marketing এবং Finance কর্মীরা সামগ্রিকভাবে বহুমুখী কার্যক্রমের মূল্য নির্ধারণের জন্য বিশ্লেষণ (analytics) ব্যবহার করে।

কোম্পানিগুলো কল সেন্টার এবং অন্যান্য পরিষেবা ও সহায়তা চ্যানেলগুলোর কার্যক্ষমতার মধ্যে আরও বেশি visibility আনায় এই ধরনের বিশ্লেষণগুলোর জনপ্রিয়তা দিন দিন বৃদ্ধি পাচ্ছে। ফলে তারা সন্তুষ্টির পর্যায়কে প্রভাবিত করার পূর্বে সমস্যাগুলো সংশোধন করতে পারে। সমর্থন-কেন্দ্রিক (support-focused) অ্যাপ্লিকেশনগুলোতে সাধারণত বিক্রয়ের জন্য অনুরূপ ড্যাশবোর্ড এবং response time, সার্ভিস কোয়ালিটি, এজেন্ট পারফরম্যান্স ও বিভিন্ন ইস্যুর ফ্রিকোয়েন্সি বিশ্লেষণ করার ক্ষমতা থাকে।

### ২.২.২.৫. সমন্বিত/সহযোগী (Integrated/Collaborative)

প্রতিষ্ঠানগুলো বিশেষত বড় প্রতিষ্ঠানগুলোর মধ্যে বিভাগগুলো নিজেদের মধ্যে সহযোগিতা ছাড়াই কাজ করার প্রবণতা রয়েছে। অতি সম্প্রতি, এই টুলস্ ও সার্ভিসগুলোর উন্নয়ন ও গ্রহন প্রতিষ্ঠানের বিক্রয়, পরিষেবা ও বিপণনের মধ্যে পারস্পরিক সহযোগিতাকে উৎসাহিত করে। এটি সহযোগিতামূলক (Collaborative) সিস্টেমের একটি ধারনা তৈরি করে, যা প্রযুক্তি ব্যবহার করে বিভাগগুলোর মধ্যে পারস্পরিক সম্পর্ক তৈরি করতে সাহায্য করে। উদাহরণস্বরূপ, একটি প্রযুক্তিগত সহায়তা কেন্দ্রের ফিডবেক বিপণনকারীদেরকে নির্দিষ্ট পরিষেবা ও পণ্যের বৈশিষ্ট্যগুলো সম্পর্কে জ্ঞান দিতে পারে। অন্যদিকে প্রতিনিধিরা একটি পৃথক এসএফএ পদ্ধতিতে রেকর্ড ও কন্টাক্ট ডেটা পুনরায় প্রবেশ করানো ছাড়াই এই সুযোগগুলো কাজে লাগাতে পারে। এই কারণে, অনেক শীর্ষস্থানীয় ও সর্বাধিক প্রচলিত পণ্যগুলো ইন্ট্রিগেটেড স্যুইট হিসাবে পাওয়া যায়।

### ২.২.৩. সিআরএম-এর জন্য সফটওয়্যার

গার্টনার (www.gartner.com) অনুসারে এসএপি, ওরাকল, সেলসফোর্স.কম, মাইক্রোসফট ও এ্যামডকস হলো সবচেয়ে বেশি বিক্রি হওয়া সফটওয়্যার।

## ২.৩। ই-মেইল সফটওয়্যার

### ২.৩.১. ই-মেইল কী?

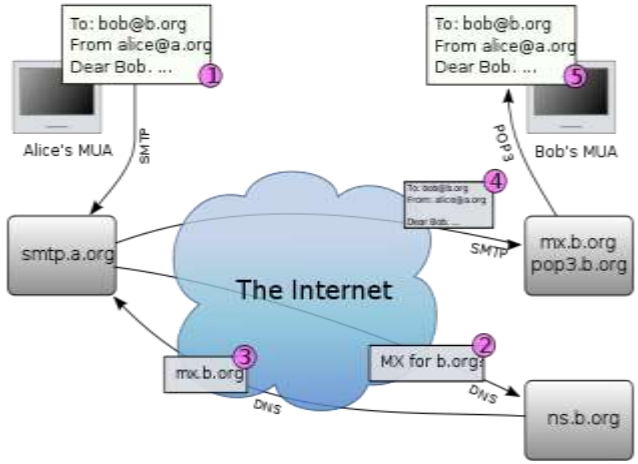
ইলেকট্রনিক মেইল (যাকে সাধারণত ইমেল বা ই-মেইলও বলা হয়) হল ইন্টারনেট বা অন্যান্য কম্পিউটার নেটওয়ার্কে ডিজিটাল বার্তা আদান-প্রদানের একটি পদ্ধতি।

একটি অফিসের মধ্যে মেল পাঠানোর প্রচলিত পদ্ধতিতে, মেলগুলো এক বিভাগ থেকে অন্য বিভাগে ব্যক্তির মাধ্যমে প্রেরণ করা হয়। এতে অনেক সময় লাগে এবং এটি ঝুঁকিপূর্ণও। এতে তথ্যের অসঙ্গতি বাড়ে। সুতরাং আমাদের একটি পদ্ধতি দরকার যা দ্রুত ও সঠিক। এটি মেইলিং সিস্টেম দ্বারা অর্জন করা যেতে পারে।

ইলেকট্রনিক মেইলিং পদ্ধতি একই সঙ্গে উভয়পক্ষের উপস্থিতি ছাড়াই স্বতঃস্ফূর্তভাবে মেইল পাঠাতে পারে। উপরন্তু একই সময়ে আরও বেশি মানুষকে মেইল পাঠানো যেতে পারে। এটি পাঠানো বার্তাগুলোর একটি লিখিত অনুলিপিও রেখে দেয়, যা ফাইল করা যেতে পারে। এটি প্রচলিত পদ্ধতির তুলনায় অনেক সস্তা।

### ২.৩.২. অপারেশন ওভারভিউ (Operation overview)

নিচের চিত্রটি ঘটনাগুলোর একটি সাধারণ ক্রম দেখায়, যা ঘটে যখন অ্যালিস তার মেইল ইউজার এজেন্ট (এমইউএ) ব্যবহার করে একটি বার্তা লেখেন। তিনি তার সংবাদদাতার ইমেল ঠিকানা প্রবেশ করেন এবং 'পাঠান' বোতামে চাপ দেন।




১. অ্যালিসের MUA বার্তাটিকে ইমেল ফর্মেটে রূপান্তর করে এবং সিম্পল মেল ট্রান্সফার এজেন্ট (SMTP) ব্যবহার করে এটিকে লোকাল মেল ট্রান্সফার এজেন্টের (MTA) এর কাছে পাঠায়। এই ক্ষেত্রে SMTP হল smtp.a.org যা অ্যালিসের ইন্টারনেট পরিষেবা প্রদানকারী (ISP) পরিচালনা করে থাকে।

২. MTA এসএমটিপি প্রোটোকলে প্রদত্ত গন্তব্য ঠিকানা দেখে (বার্তা শিরোনাম থেকে নয়), এক্ষেত্রে bob@b.org। একটি ইন্টারনেট ইমেল ঠিকানা হলো localpart@exampledomain ফর্মেটের একটি স্ট্রিং। @ চিহ্নের আগের অংশটি ঠিকানার স্থানীয় অংশ, যা সাধারণত প্রাপকের নাম হয়ে থাকে; এবং @ চিহ্নের পরে অংশটি একটি ডোমেন এর নাম বা একটি পরিপূর্ণ ডোমেন এর নাম। MTA ডোমেন নেম সিস্টেম (DNS) ব্যবহার করে মেল এক্সচেঞ্জ সার্ভারের পূর্ণাঙ্গ ডোমেন নাম নির্ধারণ করে থাকে।

৩. b.org ডোমেনের জন্য ডিএনএস সার্ভার (ns.b.org) সেই ডোমেনের অন্তর্ভুক্ত মেল এক্সচেঞ্জ সার্ভারসমূহের তালিকাসহ একটি MX রেকর্ডসহকারে সাড়া দেয়। এ ক্ষেত্রে MX রেকর্ডটি হলো mx.b.org যাহা ববের ISP পরিচালনা করে থাকে।

৪. smtp.a.org এসএমটিপিএর মাধ্যমে mx.b.org-এ বার্তা পাঠায়, যা পরবর্তীতে ববের মেলবক্সে পৌঁছে দেয়।

৫. বব তার এমইউএ-তে 'get mail' বোতাম টিপে, যা পোস্ট অফিস প্রোটোকল (POP3) ব্যবহার করে বার্তাটি এনে দেয়।

### ২.৩.৩। একটি মেসেজিং সিস্টেমের উপাদান (Components in a messaging system)

ই-মেইল আর্কিটেকচার এক বা একাধিক প্রাপকের কাছে বার্তা ও নথির ইলেকট্রিক বিতরণ করার উপায় বর্ণনা করে। নিম্নলিখিতগুলো মেল ট্রান্সফার এজেন্ট, মেল ইউজার এজেন্ট এবং গেটওয়ের মতো বিভিন্ন উপাদান ব্যবহারের জন্য ওপেন সোর্স ও বাণিজ্যিকভাবে সহজলভ্য সফ্টওয়্যারগুলোর একটি তালিকা প্রদান করে।

**১. মেল ট্রান্সফার এজেন্ট (MTA)**

ক) ওপেন সোর্স : সেন্ডমেইল (Sendmail) ই-মেইল অ্যাপ্লিকেশন সার্ভার, কিউমেল (Qmail) ই-মেইল অ্যাপ্লিকেশন সার্ভার।

খ) বাণিজ্যিক : এমএস এক্সচেঞ্জ (MS Exchange) ই-মেইল অ্যাপ্লিকেশন সার্ভার, লোটাস ডমিনো (Lotus Domino) ই-মেইল অ্যাপ্লিকেশন সার্ভার।

২. মেল ইউজার এজেন্ট (MUA)
ক) বাণিজ্যিক : লোটাস নোটস (Lotus Notes) ই-মেইল ক্লায়েন্ট, আউটলুক (Outlook) ই-মেইল ক্লায়েন্ট, আউটলুক এক্সপ্রেস (Outlook Express) ই-মেইল ক্লায়েন্ট, ইউডোরা (Eudora) ই-মেইল ক্লায়েন্ট।

৩. গেটওয়ে
ক) বাণিজ্যিক : লোটাস মেসেজ (Lotus Message Switch) সুইচ ই-মেইল গেটওয়ে, আউটলুক ওয়েব অ্যাক্সেস (OutlookWeb Access) ই-মেইল গেটওয়ে।

### ২.৩.৪. জনপ্রিয় ই-মেইল সিস্টেম (Popular E-mail Systems)

#### ২.৩.৪.১. সেন্ড মেইল (Send Mail)
সেন্ডমেল হলো একটি সাধারণ-পারফাস ইন্টারনেটওয়ার্ক ইমেল রাউটিং সুবিধা, যা ইন্টারনেটে ইমেইল পরিবহনের জন্য ব্যবহৃত সাধারণ মেল ট্রান্সফার প্রোটোকল (এসএমটিপি) সহ অনেক ধরনের মেল ট্রান্সফার ও বিতরণ পদ্ধতি সমর্থন করে।

#### ২.৩.৪.২. কিউমেল (Qmail)
কিউমেল হলো একটি মেল ট্রান্সফার এজেন্ট (এমটিএ) যা ইউনিক্সে চলে। এটি জনপ্রিয় সেন্ডমেইল প্রোগ্রামের একটি বিকল্প প্রতিস্থাপন হিসাবে ড্যানিয়েল জে. বার্নস্টেইন ১৯৯৫ সালের ডিসেম্বর মাসে লিখতে শুরু করেন। Qmail এর সোর্স কোড পাবলিক ডোমেনে রয়েছে, ফলে Qmail একটি ফ্রি সফটওয়্যার।

#### ২.৩.৪.৩. মাইক্রোসফট এক্সচেঞ্জ সার্ভার : (Microsoft Exchange Server)
মাইক্রোসফ্ট এক্সচেঞ্জ সার্ভার হলো একটি ক্লায়েন্ট-সার্ভারের সার্ভার সাইট প্রোগ্রাম যাহা মাইক্রোসফ্ট দ্বারা তৈরি একটি সহযোগী অ্যাপ্লিকেশন প্রোডাক্ট। এটি সার্ভার লাইনের মাইক্রোসফ্ট সার্ভারের একটি অংশ ও মাইক্রোসফ্ট অবকাঠামো পণ্য ব্যবহার করে এমন প্রতিষ্ঠানগুলো ব্যবহার করে থাকে। এক্সচেঞ্জ এর প্রধান বৈশিষ্ট্যগুলো হলো ইলেকট্রনিক মেল, ক্যালেন্ডারিং, কন্টাক্ট ও টাস্ক, তথ্যে মোবাইল ও ওয়েবভিত্তিক অ্যাক্সেসের সুবিধা, এবং তথ্য স্টোরেজের সাপোর্ট।

#### ২.৩.৪.৪. লোটাস ডমিনো (Lotus Domino)
আইবিএম লোটাস ডোমিনো সফ্টওয়্যার হল ক্রিটিক্যাল ব্যবসা, সহযোগিতা ও মেসেজিং অ্যাপ্লিকেশনের জন্য একটি বিশ্বমানের প্ল্যাটফর্ম।

### ২.৩.৫. বাণিজ্যিক প্রডাক্টের লাইসেন্সিং (Licensing of Commercial Product)

#### ২.৩.৫.১. এক্সচেঞ্জ সার্ভার : (Exchange Server)
এক্সচেঞ্জ সার্ভারের ক্ষেত্রে সার্ভার/ক্লায়েন্ট অ্যাক্সেস লাইসেন্স (CAL) মডেলে লাইসেন্স প্রদান করা হয়। যে সমস্ত সার্ভারে এই সফ্টওয়্যার চালানো হচ্ছে, তার প্রতিটির জন্য একটি করে লাইসেন্স ক্রয় করতে হয়। যে সমস্ত ইউজার বা ডিভাইস সার্ভার সফ্টওয়্যার অ্যাক্সেস করে তার প্রতিটির জন্য এক্সচেঞ্জেরও একটি CAL লাইসেন্সের প্রয়োজন হয়। একচেঞ্জের জন্য দুই ধরনের CAL লাইসেন্স রয়েছে :

স্ট্যান্ডার্ড CAL : ব্যবহারকারীদের যেকোনো প্ল্যাটফর্ম, ব্রাউজার, বা মোবাইল ডিভাইস থেকে আরও বেশি উৎপাদনশীল হতে সাহায্য করার উদ্দেশ্যে এটি ডিজাইন করা হয়েছে। এক্সচেঞ্জ সার্ভার ২০১০-এ এই সমস্ত নতুন বৈশিষ্ট্য সংযোগ করা হয়েছে, যা যোগাযোগে ওভারলোড এবং কম খরচে হেল্পডেস্ক ম্যানেজ করতে সহায়তা করে।

এন্টারপ্রাইজ CAL : নতুন সমন্বিত আর্কাইভিং ফাংশনালিটি ও তথ্য সুরক্ষা ক্যাপাবিলিটির কমপ্লায়েন্স পূরণের খরচ এবং জটিলতা হ্রাসের উদ্দেশ্যে ডিজাইন করা হয়েছে। পাশাপাশি লেগাসি (Legacy) ভয়েস মেইল সিস্টেমকে ইউনিফায়েড ম্যাসেজিং দ্বারা প্রতিস্থাপন করে ব্যবহারকারীদের খরচ কমাতে সহায়তা করে।

ব্যবহারকারীদের সার্ভার সফ্টওয়্যার মাইক্রোসফ্ট আউটলুক ও ফোরফ্রন্ট (Forefront) অনলাইন সিকিউরিটি সিস্টেমসমূহের জন্যও লাইসেন্স ক্রয় করতে হয়।

#### ২.৩.৫.২. লোটাস ডমিনো (Lotus Domino)
আইবিএম লোটাস নোটস এবং ডোমিনো সফ্টওয়্যার এর লাইসেন্স ক্রয়ের জন্য IBM তিনটি অপশন দেয়—যাতে ব্যবহারকারীরা তাদের পছন্দ অনুযায়ী এবং তাদের প্রয়োজনীয় কার্যাবলি ও শিথিলতা অনুযায়ী লাইসেন্স ক্রয় করতে পারে।

ব্যবহারকারীরা যদি গ্রাহক ও সার্ভার লাইসেন্সিং অপশনটি পছন্দ করেন, তবে তারা তাদের সার্ভার মেশিনের সঙ্গে যুক্ত প্রসেসর ইউনিটের মান ও প্রতি ইউজারের জন্য CAL অনুযায়ী নির্ধারিত সংখ্যক লাইসেন্স ক্রয় করবেন।

ব্যবহারকারীরা যদি পার ইউজার লাইসেন্সিং (Per user licensing) পছন্দ করেন, তাহলে তারা তাদের সংস্থার আকারের ওপর ভিত্তি করে প্রতি ব্যবহারকারীর জন্য চার্জ প্রদান করে। এক্ষেত্রে তাদের আইবিএম লোটাস ডোমিনো সার্ভার ও ক্লায়েন্ট অ্যাক্সেস অপশনগুলোর যেকোনো সমন্বয় স্থাপনের সুযোগ রয়েছে।

ব্যবহারকারীরা যদি তাদের কোম্পানির বাইরে ও ভেতরে উভয় ধরনের অ্যাক্সেসের জন্য Collborative অ্যাপ্লিকেশন হোস্ট করতে চান, কিন্তু মেইল ও ক্যালেন্ডার-এর প্রয়োজন নেই, সেক্ষেত্রে 'Processor Value Unit Licensing' তাদের জন্য সবচেয়ে সাশ্রয়ী হতে পারে।

উভয় ক্ষেত্রে, ব্যবহারকারীরা যদি ইমেইল সিকিউরিটি অ্যাপ্লায়েন্স-এর অতিরিক্ত কম্পোনেন্ট স্থাপন করতে চান, তাহলে এটি সামগ্রিক পদ্ধতিতে অতিরিক্ত লাইসেন্সিং খরচ যোগ করবে।

## ২.৪. অ্যান্টিভাইরাস সফটওয়্যার (Anti-virus software)

### ২.৪.১. অ্যান্টিভাইরাস সফটওয়্যার কী?

অ্যান্টিভাইরাস সফ্টওয়্যার হলো একটি কম্পিউটার প্রোগ্রাম, যা ভাইরাস এবং ওয়ার্মের মতো দূষিত (malicious) সফ্টওয়্যার প্রোগ্রামগুলোকে চিহ্নিত করে, প্রতিরোধ করে এবং অপসারণ করতে প্রয়োজনীয় ব্যবস্থা নেয়। আপনি অ্যান্টিভাইরাস সফ্টওয়্যার ব্যবহার করে আপনার কম্পিউটারকে ভাইরাসমুক্ত করতে পারেন।

কম্পিউটার ভাইরাস হলো এমন সফ্টওয়্যার প্রোগ্রাম যা ইচ্ছাকৃতভাবে কম্পিউটার অপারেশনে হস্তক্ষেপ করতে, রেকর্ড করতে, নষ্ট করতে বা তথ্য মুছে ফেলতে অথবা অন্য কম্পিউটারে ও ইন্টারনেটজুড়ে নিজেদের ছড়িয়ে দিতে তৈরি করা হয়েছে।

অতীতে পিসিগুলো প্রধানত ভাইরাস ও জীবাণু দ্বারা আক্রমণের হুমকির মধ্যে ছিল। এসব কর্মসূচির মূল উদ্দেশ্য ছিল প্রসার (spread); কিন্তু, কিছু প্রোগ্রাম নথি ও কম্পিউটার ক্ষতিগ্রস্ত করতে ডিজাইন করা হয়েছে। এই ধরনের ক্ষতিকারক সফ্টওয়্যার, বা 'ম্যালওয়্যার'-কে 'Cyber Vandalism' হিসাবে বর্ণনা করা যেতে পারে। বেশিরভাগ ক্ষেত্রে, ভাইরাস ও জীবাণুর লক্ষ্য ছিল যতটা সম্ভব ছড়িয়ে দেওয়া, যাতে উচ্চ সংক্রমিত হয়, ফলে প্রোগ্রামটি প্রচুর খ্যাতি অর্জন করতে পারে।

কিন্তু সাম্প্রতিক বছরগুলোতে পরিস্থিতির ব্যাপক পরিবর্তন হয়েছে। আজ কম্পিউটারের সবচেয়ে বড় হুমকি হলো ক্রাইমওয়্যার (crime ware)। এই বিপজ্জনক সফ্টওয়্যারটি সাইবার অপরাধীরা অবৈধভাবে অর্থোপার্জনের উদ্দেশ্যে লিখেছে। ক্রাইম ওয়ার ভাইরাস, ওয়ার্ম, ট্রোজান বা অন্যান্য খারাপ প্রোগ্রামের রূপ নিতে পারে।

সাম্প্রতিক ভাইরাস প্রতিরোধে আমাদের অবশ্যই নিয়মিত অ্যান্টিভাইরাস সফ্টওয়্যার হালনাগাদ করতে হবে। বর্তমানে আমরা এমন ধরনের অ্যান্টিভাইরাস সফ্টওয়্যার সংস্থাপন করতে পারি যা স্বয়ংক্রিয়ভাবে আপডেট হতে পারে।

### ২.৪.২. অ্যান্টিভাইরাস কীভাবে কাজ করে?

অ্যান্টিভাইরাস ভাইরাস সনাক্ত করতে বেশ কয়েকটি কৌশল ব্যবহার করে। সেগুলো হলো—

#### ২.৪.২.১. স্বাক্ষরভিত্তিক শনাক্তকরণ (Signature-based detection)

এটি অভিধান পদ্ধতি হিসাবেও পরিচিত। প্রতিটি ভাইরাসের আক্রমণের নিজস্ব উপায় আছে। আক্রমণের স্বাক্ষর একটি অ্যান্টিভাইরাস ডাটাবেসে সংরক্ষণ করা হয়। ভাইরাস শনাক্ত করতে, অ্যান্টিভাইরাস সফ্টওয়্যার একটি ফাইলের বিষয়বস্তুকে সংরক্ষিত ভাইরাস স্বাক্ষরের অভিধানের সঙ্গে তুলনা করে। যদি ফাইলের নির্দেশনার একটি অংশ অভিধানে চিহ্নিত কোনো ভাইরাসের সঙ্গে মিলে যায়, তাহলে অ্যান্টি-ভাইরাস সফ্টওয়্যারটি হয় ফাইলটি মুছে ফেলতে পারে, নতুবা এটিকে আলাদা করে রাখতে পারে (quarantine) যাতে ফাইলটি অন্য প্রোগ্রামে অ্যাক্সেস নিতে না পারে এবং ভাইরাসটি ছড়িয়ে পড়তে না পারে বা ফাইল থেকে ভাইরাস নিজেই অপসারিত হয়ে তা মেরামত করার চেষ্টা করতে না পারে। স্বাক্ষরভিত্তিক শনাক্তকরণের জন্য, অ্যান্টিভাইরাস সফ্টওয়্যারকে সাম্প্রতিক ভাইরাস স্বাক্ষর ডাটাবেসের সঙ্গে আপডেট করতে হবে। অ্যান্টিভাইরাস ইন্টারনেট থেকে আপডেট নিতে পারে বা অ্যান্টিভাইরাস কোম্পানির দেওয়া সর্বশেষ প্যাচ ইনস্টল করে তা আপডেট করা যেতে পারে।

#### ২.৪.২.২. আচরণভিত্তিক শনাক্তকরণ (Behaviour-based detection)

অ্যান্টিভাইরাস হোস্ট বা পিসিতে অস্বাভাবিক আচরণ শনাক্ত করে। কৌশলটি এই ধারণা থেকে আসে যে আক্রমণগুলো একটি ফাইলের 'স্বাভাবিক' (বৈধ) কার্যকলাপ থেকে আলাদা এবং তাই এই দুইয়ের পার্থক্য থেকে অনুপ্রবেশ শনাক্ত করা হয়। যদি একটি প্রোগ্রাম একটি executiable প্রোগ্রামে ডেটা লেখার চেষ্টা করে, তাহলে, এটি একটি সন্দেহজনক আচরণ হিসাবে চিহ্নিত করা হয় এবং ব্যবহারকারীকে এই বিষয়ে সতর্ক করা হয় এবং কী করতে হবে তা জানতে চাওয়া হয়।

অ্যান্টিভাইরাস শুধু ইউজারের কম্পিউটারে ইনস্টল ও রক্ষণাবেক্ষণ করা যায় এবং ইন্টারনেট থেকে হালনাগাদ করা যায়। তাছাড়া ল্যান পরিবেশে, অ্যান্টিভাইরাসের ক্লায়েন্ট সফটওয়্যার ইউজারের কম্পিউটারে ইনস্টল করা হয়

এবং সার্ভার থেকে তা পরিচালিত হয়। এক্ষেত্রে সার্ভার ইন্টারনেট থেকে সাম্প্রতিক আপডেট নেয় এবং ক্লায়েন্ট কম্পিউটারগুলোতে সাম্প্রতিক আপডেট বিতরণ করে।

### ২.৪.৩. লাইসেন্সিং/(Licensing)

বেশিরভাগ বাণিজ্যিক অ্যান্টিভাইরাস সফ্টওয়্যারের এন্ড ইউজার লাইসেন্স চুক্তিটি এক বছরের জন্য করা হয়। লাইসেন্সের মেয়াদ শেষ হওয়ার ৩০ থেকে ৬০ দিন পূর্বে ব্যবহারকারীকে নবায়নের জন্য বলা হয়। ক্রেতারা একটি নতুন লাইসেন্সের বিপরীতে একটি নির্দিষ্ট অংকের অর্থ পরিশোধ করে এবং অ্যান্টিভাইরাস কোম্পানি থেকে একটি নতুন অ্যাক্টিভেশন কোড বা সিরিয়াল নম্বর পান। অ্যান্টিভাইরাস 'ভাইরাস স্বাক্ষর ডাটাবেস' হালনাগাদ করতে ব্যর্থ হয় যদি লাইসেন্সটি নবায়ন না করা হয় এবং সেক্ষেত্রে নতুন ভাইরাসের আক্রমণের বিরুদ্ধে কম্পিউটারের নিরাপত্তা আপস করে। কিছু অ্যান্টিভাইরাস প্রোগ্রাম বিনামূল্যে ডাউনলোড করা যায়, কিন্তু এগুলো অন্যান্য বাণিজ্যিক অ্যান্টিভাইরাসের মতো কার্যকর নয়।

### ২.৪.৪. জনপ্রিয় অ্যান্টিভাইরাস প্রোগ্রাম

বাজারে বেশ কিছু জনপ্রিয় অ্যান্টিভাইরাস পাওয়া যায় যেমন ম্যাকাফি, ক্যাসপারস্কি, NOD32, অ্যাভাস্ট, AVG, ইত্যাদি। কিছু অ্যান্টিভাইরাস কোম্পানি অ্যান্টিভাইরাস সফ্টওয়্যারের অংশ হিসাবে ওয়েব নিরাপত্তা, ইমেইল নিরাপত্তা, ডেস্কটপ ব্যবস্থাপনা, পিসি সলিউশন, আইডিএস (Intrusion Detection System) ও ফায়ারওয়াল প্রদান করে। উদাহরণস্বরূপ, ক্যাসপারস্কি অ্যান্টিভাইরাস ফায়ারওয়াল ও ইমেল সুরক্ষাসহ আসে। কখনও কখনও অ্যান্টিভাইরাস সফ্টওয়্যারে প্রতিটি নতুন মডিউল যোগ করার জন্য অতিরিক্ত ফি দাবি করা হয়।

## ২.৫. অ্যান্টি-ম্যালওয়্যার সফ্টওয়্যার (Anti-malware software)

ম্যালওয়্যার একটি নেটওয়ার্কে একটি স্ট্যান্ড-এলোন কম্পিউটার বা পিসির ক্ষতি করতে ডিজাইন করা হয়। তাই যখনই ম্যালওয়্যার শব্দ ব্যবহার করা হয় তখন তাহা এমন একটি প্রোগ্রামকে বোঝায়, যা একটি কম্পিউটার পদ্ধতিকে ক্ষতিগ্রস্ত করতে তৈরি করা হয়েছে—এটি একটি ভাইরাস, ওয়ার্ম বা ট্রোজান হতে পারে।

ভাইরাস হলো এমন একটি প্রোগ্রাম, যা ব্যবহারকারীর অনুমতি ছাড়াই অন্যান্য প্রোগ্রামে (অপারেটিং সিস্টেমসহ) সংযুক্ত হয়ে যায় এবং যখন এই প্রোগ্রামটি চালানো হয় তখন ভাইরাসটি অন্যান্য প্রোগ্রামে ছড়িয়ে পড়ে।

ওয়ার্ম হলো একটি স্ট্যান্ড-এলোন ম্যালওয়্যার প্রোগ্রাম, যা সক্রিয়ভাবে অন্য কম্পিউটারকে সংক্রমিত করতে একটি নেটওয়ার্কের মাধ্যমে নিজেকে প্রেরণ করে।

ট্রোজান সাধারণত অন্য ফাইলে বা প্রোগ্রামে নিজেকে যুক্ত করার চেষ্টা করে না বা অন্যথায় নিজেদের প্রকাশ করে না। এটি ভিকটিমের কাছে খুবই জরুরি রুটিন বা আকর্ষণীয় বলে নিজেকে উপস্থাপন করে, যাতে ভিকটিম এটি ইনস্টল করতে উদ্বুদ্ধ হয়।

অ্যান্টি-ম্যালওয়্যার সফ্টওয়্যার হলো এক ধরনের সফ্টওয়্যার প্রোগ্রাম, যা কম্পিউটার পদ্ধতিকে ক্ষতিকারক সফ্টওয়্যার বা ম্যালওয়্যার থেকে রক্ষা করতে তৈরি করা হয়েছে। অ্যান্টি-ম্যালওয়্যার প্রোগ্রাম ম্যালওয়্যার প্রতিরোধ, শনাক্ত ও অপসারণ করতে একটি কম্পিউটার সিস্টেমকে স্ক্যান করে।

অ্যান্টিভাইরাস সফ্টওয়্যার একটি সিস্টেম থেকে ভাইরাস এবং অন্যান্য বিপজ্জনক সফ্টওয়্যার শনাক্ত ও অপসারণ করতে তৈরি করা হয়েছে, যেখানে অ্যান্টি-ম্যালওয়্যার সফ্টওয়্যার এমন একটি প্রোগ্রাম, যা ভাইরাস, ট্রোজান ও ওয়ার্মসহ সমস্ত ধরনের ম্যালওয়্যারের সংক্রমণ থেকে সিস্টেমকে রক্ষা করে।

ম্যাকাফি, নর্টন, ক্যাসপারস্কি, ওয়েবরুট, অ্যাভাস্ট ও ট্রেন্ড মাইক্রো হলো বাণিজ্যিকভাবে প্রাপ্ত অ্যান্টি-ম্যালওয়্যার সফ্টওয়্যার।

## পর্যালোচনামূলক প্রশ্নাবলি

**1. Multiple Choice Questions (MCQ)**

i) Which of the following is not an instrument cleared through a clearing house?

a) Cheque b)Pay Order c) Dividend d) Gift Voucher

ii) Which of the following is not a part of clearing system?

a) RTGS b) BACH c) BACPS d) ERP

iii) Which of the following is not a component of an ERP system?

a) Manufacturing b) Supply Chain Management c) Human Resources d) Credit Card

iv) Which of the following is not an e-mail system?

a) Sendmail b) Lotus Domino c) Active-Passive Server d) Microsoft Exchange Server

**2. Fill in the gap(s)**

i) BACPS stands for —and BEFTN stands for—

ii) BACPS was launched by the Bangladesh Bank in -----

iii) At presnt, —number of clearing systems are operating in Bangladesh

iv) The first clearing starts at—and the returns of the same occur at—.

v) MICR stands for —

vi) The major MICR fonts used around the world are—and—

vii) For clearing purpose, Bangladesh Bank provided all Banks a software called—

## সম্ভাব্য প্রশ্নাবলি

1. What is a Cheque Processing System?
2. Name four clearing systems that are in operation in Bangladesh.
3. Narrate the conventional cheque clearing process.
4. Define MICR, Cheque Truncation and RTGS.
5. What is BACH? What are the two parts of BACH? Narrate them.
6. What is a large value cheque settlement? How this is different than the normal cheque settlement?
7. What are the current timing in force for different clearing systems?
8. How MICR differs from a bar code?
9. How cheque truncation helps to stop physical movement of cheque?
10. What is PBM or participating Bank module in clearing system?
11. What are the benefits of a cheque truncation system over a traditional cheque clearing system?
12. What is the basic difference between RTGS and BEFTN?
13. What is routing number? What are the significance of digits of a routing number?
14. Why ERP software is used in banks?
15. Name a few components or modules of an ERP system.
16. Name two renowned commercial ERP software. Who are manufacturer of them?
17. Why a CRP software is used in a bank?

18. Brief in short the fields of application of a CRM software.
19. Narrate the importance of an email software.
20. Narrate in brief the four commercially used email systems?
21. Write the licensing policy of Exchange Server or Lotus Domino.
22. What is the difference between Virous and Malware? Name a few available Virus and Malware.
23. How an anti-virus software and an anti-malware software differs from each other?
24. Name five of each of the anti-virus software and an anti-malware software.

মডিউল-এফ

# ফিনটেক, কৃত্রিম বুদ্ধিমত্তা এবং ভবিষ্যৎ প্রযুক্তিভিত্তিক ব্যাংকিং

## ১. ফিনটেক, র‍্যাগটেক ও টেকফিন (FinTech, RegTech and TechFin)

ব্যাংকিং ও প্রযুক্তির মধ্যে ইন্টারেকশন পারস্পরিক শক্তিবৃদ্ধির একটি দীর্ঘ ইতিহাস রয়েছে এবং উভয়ের সঙ্গে জড়িত ব্যক্তিদের দ্বারা অনেক প্রশংসিত হয়েছে। ফিনটেক, র‍্যাগ টেক এবং টেকফিন হল এই ধরনের কিছু সহযোগিতা, যা এখনও পর্যন্ত আশ্চর্যজনক প্রোডাক্ট তৈরিতে সফল হয়েছে।

### ১.১. ফিনটেক (FinTech)

ফিন্যান্সিয়াল টেকনোলজি (ফিনটেক) হলো সেই প্রযুক্তি ও উদ্ভাবন, যার লক্ষ্য আর্থিক পরিষেবা প্রদানের ক্ষেত্রে প্রথাগত আর্থিক পদ্ধতির সঙ্গে প্রতিযোগিতা করা। ব্যাংক, লিজিং কোম্পানি এবং বীমা কোম্পানির মতো আর্থিক কোম্পানি যারা তাদের নিজস্ব প্রোডাক্টকে আরও আকর্ষণীয় করে তুলতে চায় তারা ফিনটেক ব্যবহার করে। অনলাইন ব্যাংকিং, ইন্টারনেট ব্যাংকিং, ডেবিট কার্ড, ক্রেডিট কার্ড, এটিএম/সিআরএমএম, এমএফএস, এজেন্ট ব্যাংকিং ও মোবাইল অ্যাপস্ ইত্যাদি ব্যাংকের জন্য ব্যবহৃত কিছু ফিনটেকের উদাহরণ। ফিনটেক ব্যবহারে গ্রাহক সেবা যথেষ্ট উন্নত হয়েছে এবং যে ব্যাংকগুলো ফিনটেক প্রথম গ্রহণ করেছে তারা অন্যদের থেকে এগিয়ে রয়েছে।

বাংলাদেশে ফিনটেক ব্যবহার করে প্রদেয় সবচেয়ে সুপরিচিত সমাধান হলো নেক্সাসপে, সিটিটাচ্, আস্থা, সেলফিন, মাইপ্রাইম, ইবিএল স্কাই ব্যাংকিং, এমটিবি স্মার্ট ব্যাংকিং, রকেট, বিকাশ, নগদ, ইউপে, এসএসএলকমার্জ, আইফার্মার, পেওয়েল, ডিমানি, ইত্যাদি।

### ১.২ টেকফিন (TechFin)

টেকফিন হলো টেকনোলজি কোম্পানি, যার প্রধান রেভিন্যু আসে প্রযুক্তিগত প্রোডাক্ট থেকে। তারা তাদের মূল ব্যবসা থেকে প্রচুর পরিমাণে গ্রাহকের ডেটা সংগ্রহ করেছে এবং এখন ঐ সমস্ত গ্রাহকের ডেটা ব্যবহার করে ফাইন্যান্সিয়াল সার্ভিস চালাতে চায়। টেকফিন কোম্পানির উদাহরণ হলো, ফেসবুকের মতো

সোশ্যাল মিডিয়া কোম্পানি, গুগলের মতো সার্চ ইঞ্জিন, অ্যামাজনের মতো ই-কমার্স কোম্পানি, গস্থামীণফোন, রবি ও বাংলালিংকের মতো টেলিযোগাযোগ কোম্পানি, এবং আইবিএম ও ডেলের মতো হার্ডওয়্যার কোম্পানি। তারা একটি বীমা পলিসির মূল্য নির্ধারণের জন্য, নির্দিষ্ট লোন প্রোডাক্টের জন্য সম্ভাব্য গ্রাহকদের খুঁজে পেতে, বা গ্রাহকের ক্রেডিট স্কোর মূল্যায়ন করতে তাদের কাছে সংগৃহীত ডেটা ব্যবহার করে।

বাংলাদেশের টেলিযোগাযোগ কোম্পানিগুলো তাদের নিজস্ব গ্রাহকদের জন্য তাদের বিদ্যমান ডিস্ট্রিবিউশন চ্যানেল বা একটি নিও লোন প্রোডাক্ট ব্যবহার করে একটি MFS চালু করতে পারে। এক্ষেত্রে গ্রাহক ও লোনের পরিমাণ গ্রাহকদের দ্বারা নেটওয়ার্কের ব্যবহারের ধরন ও পেমেন্টের ধরন অনুযায়ী নির্ধারিত হতে পারে।

### ১.৩. র‍্যাগটেক (RegTech)

রেগুলেটরি প্রযুক্তি (Regulatory Technology) র‍্যাগটেক নামে পরিচিত। র‍্যাগটেক হলো বর্তমানে বিশ্বব্যাপী আর্থিক এবং কমপ্লায়েন্স সম্প্রদায়ে ব্যবহৃত একটি বাজ্ওয়ার্ড। র‍্যাগটেক শব্দটি প্রথম ২০১৫ সালে যুক্তরাজ্যের ফিন্যান্সিয়াল কন্ডাক্ট অথরিটি (এফসিএ) দ্বারা ব্যবহার করা হয়েছিল। তাদের সংজ্ঞা অনুসারে, এটি ফিনটেকের একটি সাবসেট, যা প্রযুক্তির ওপর গুরুত্বারোপের মাধ্যমে বিদ্যমান দক্ষতার তুলনায় আরও বেশি দক্ষতার সঙ্গে এবং কার্যকরভাবে নিয়ন্ত্রণ সংস্থার কার্যাবলি পরিচালনা করতে পারে।

সহজভাবে, এটি এমন কোনো প্রযুক্তিকে বোঝায়, যা কোম্পানিগুলোকে তাদের নিয়ন্ত্রক সংস্থার নিয়ম মেনে চলা নিশ্চিত করে। র‍্যাগটেকের একটি নিখুঁত উদাহরণ হল ইলেকট্রনিক নো ইয়োর কাস্টমার (ই-কেওয়াইসি) প্রক্রিয়া—যার মাধ্যমে ব্যাংকগুলো ডিজিটাল পদ্ধতিতে অ্যাকাউন্ট খোলার সময় গ্রাহকের পরিচয় নিশ্চিত করে।

## ২. বেসিক ক্রিপ্টো কারেন্সি ও ব্লক চেইন প্রযুক্তি (Basic Crypto Currency and block chain Technology)

### ২.১ ব্লক চেইন প্রযুক্তি (Block Chain Technology)

একটি ব্লকচেইন হলো একটি ডিস্ট্রিবিউটেড ডাটাবেস বা লেজার যেখানে তথ্য ইলেকট্রনিকভাবে ডিজিটাল পদ্ধতিতে সংরক্ষণ করা হয় এবং একটি কম্পিউটার নেটওয়ার্কের নোডগুলোর মধ্যে শেয়ার করা হয়। এটি তথ্য সংরক্ষণের জন্য সবচেয়ে নিরাপদ প্রযুক্তিগুলোর মধ্যে একটি।

ব্লকচেইন হলো অপরিবর্তনীয় ও নেটওয়ার্কে যে কারও কাছে দৃশ্যমান। এটি ডেটাসমূহ একসঙ্গে একটি গ্রুপে সংরক্ষণ করে। এটাকে ব্লক বলে, যার নির্দিষ্ট স্টোরেজ ক্ষমতা রয়েছে। যখন একটি ব্লক তথ্য দিয়ে পূর্ণ হয় তখন টাইমস্ট্যাম্পসহ একটি হ্যাশ দিয়ে তা বন্ধ করা হয় এবং পূর্বের ব্লকগুলোর সঙ্গে যুক্ত করা হয় এবং তা একটি নতুন হ্যাশ তৈরি করে। সমস্ত নতুন ডেটা একই পদ্ধতিতে যোগ করা হয়, এভাবে ব্লকচেইন তৈরি হয় এবং চেইনগুলোর মধ্যে থাকা ব্লকগুলোকে মুছে ফেলা, পরিবর্তন করা বা ধ্বংস করা থেকে রক্ষা করা হয়। এভাবেই ব্লকচেইন প্রযুক্তি অপরিবর্তনীয় (irreversible) হয়ে যায়।

দুই ধরনের ব্লকচেইন নেটওয়ার্ক রয়েছে, যথা—পাবলিক নেটওয়ার্ক এবং প্রাইভেট নেটওয়ার্ক। পাবলিক নেটওয়ার্কের নোডগুলো বিকেন্দ্রীভূত ও পাবলিক নেটওয়ার্কের মধ্যে বিতরণ করা হয়। নেটওয়ার্কের প্রতিটি সদস্য সমস্ত ডেটা দেখতে পারে। ইউজারগণ বেনামি এবং লেনদেনের ওপর কোনো রেগুলেশন বা নিয়ন্ত্রণ নেই। তবে ডেটা অপরিবর্তনীয়। অন্যদিকে প্রাইভেট নেটওয়ার্কে কেন্দ্রীভূত (centralized) নোড রয়েছে, যেখানে ডেটা প্রাইভেট, লেনদেনের ওপর যথেষ্ট নিয়ন্ত্রণ রয়েছে, কিন্তু ডেটা কম সুরক্ষিত।

যদিও প্রথম ১৯৯১ সালে একটি গবেষণাপত্রে এই প্রযুক্তির রূপরেখা দেওয়া হয়েছিল কিন্তু এর প্রথম রিয়েল ওয়াল্ড অ্যাপ্লিকেশনটি জানুয়ারি ২০০৯ সালে বিটকয়েন চালু করার মাধ্যমে শুরু হয়েছিল। রেকর্ড সংরক্ষণের ধরনের কারণে, যথা পাবলিক নেটওয়ার্কে ব্লকচেইন প্রযুক্তিতে লেনদেন ও সংরক্ষিত রেকর্ডসমূহ অপরিবর্তনীয় হওয়ায় অর্থাৎ রেকর্ড পরিবর্তন করা, মুছে ফেলা বা ধ্বংস করা যায় না, যার জন্য এই প্রযুক্তিটি ডিস্ট্রিবিউটেড লেজার প্রযুক্তি (DLT) নামেও পরিচিত।

ধারণা করা হচ্ছে যে, শিল্পগুলোর ডেটার ওপর কঠোর নিয়ন্ত্রণের প্রয়োজনে যেমন ব্যাংকিং ও ফাইনান্স, মুদ্রা, বীমা, স্টক মার্কেট, রেমিট্যান্স, সম্পত্তি নথিকরণ, স্বাস্থ্যসেবা, সাপ্লাই চেইন, ভোটিং পদ্ধতি, ইত্যাদিতে ব্যবহৃত ডেটার অপরিবর্তনীয় পকৃতির কারনে ভবিষ্যতে ব্লকচেইন প্রযুক্তির ব্যবহারে আগ্রহ বৃদ্ধি পাবে। বর্তমানে ক্রিপ্টোকারেন্সি প্রযুক্তিতে ব্লকচেইন প্রযুক্তি বহুলভাবে ব্যবহৃত হচ্ছে।

বাংলাদেশের প্রেক্ষাপটে, সমস্ত ব্যাংক এবং এনবিএফআই গুলোর মধ্যে দ্রুত লেনদেন প্রক্রিয়াকরণ পদ্ধতি যেমন রিয়েল-টাইম বাচ (BACH) পরিচালনার জন্য বিকেন্দ্রীভূত নোডগুলো ব্যাংক ও এনবিএফআইর মধ্যে বিতরণ করে ব্যবহার করা যেতে পারে। এটি স্টক এক্সচেঞ্জের বিভিন্ন স্টেকহোল্ডার যেমন ব্যাংক ও লিস্টেড কোম্পানির মধ্যে ডিস্ট্রিবিউটেড নোডগুলো বিতরণ করে স্টেকহোল্ডারদের ডেটা প্রক্রিয়াকরণ ও স্টকহোল্ডাদের রিয়েল টাইমে হালনাগাদ করতে ব্যবহার করা যেতে পারে। এটি গ্রাহকের অর্থ অন্যদের দ্বারা অননুমোদিত ব্যবহার থেকে প্রতিরোধ

করতে দেশব্যাপী এমএফএসের একটি একক নেটওয়ার্ক তৈরি ও পরিচালনা করতেও ব্যবহার করা যেতে পারে। একইভাবে, দেশব্যাপী স্বাস্থ্যসেবা, সরকারি সংগ্রহ পরিষেবা, সম্পত্তির নথি ব্যবস্থাপনা এবং আরও অনেক কিছুতে ব্লকচেইন প্রযুক্তি ব্যবহার করা যেতে পারে।

## ২.২. মৌলিক ক্রিপ্টো মুদ্রা (Basic Cryto Currency)

### ২.২.১. কেন ক্রিপ্টো-কারেন্সি?

সাতোশি নাকামোতো (Satoshi Nakamoto) বিদ্যমান মুদ্রা এবং কেন্দ্রীয় বা স্টেট ব্যাংক যেভাবে এটি পরিচালনা করছে তাতে খুশি ছিলেন না। ফ্রেডরিখ ফন হায়েক (Friedrich Von Hayek) তার বই 'ডিন্যাশনালাইজেশন অব মানি : দ্য আর্গুমেন্ট রিফাইন্ড' তে কেন্দ্রীয় ব্যাংকের একচেটিয়া আধিপত্যের অবসান ঘটাতে অর্থের উৎপাদন, বিতরণ ও ব্যবস্থাপনায় একটি সম্পূর্ণ মুক্ত বাজারের পক্ষে কথা বলেছেন।

এভাবেই ক্রিপ্টো-কারেন্সির ধারণার উদ্ভব হয় এবং এভাবেই জনসাধারণের উদ্বেগ কমানোর কথা ভাবতে শুরু করা হয়।

### ২.২.২. সাতোশি নাকামোতো কে? (who is Satoshi Nakamoto?)

- তিনি ব্লকচেইন প্রযুক্তি ব্যবহার করে বিটকয়েন বিশ্বের প্রথম এবং সবচেয়ে জনপ্রিয় ক্রিপ্টোকারেন্সি (২০০৯ সালে) আবিষ্কার করেন। নাকামোতো একজনের ছদ্মনাম, একজন জাপানি নাগরিক, বিটকয়েন আবিষ্কার করার সময় যার বয়স ৩০-এর দশকের শেষের দিকে ছিল বলে জানা যায়।
- অপেশাদার গোয়েন্দাদের দলগুলো আসল ব্যক্তিকে খুঁজে বের করার চেষ্টা করছে, কিন্তু এখন পর্যন্ত সফল হতে পারেনি।
- তিনি ২০১০ সালে অদৃশ্য হওয়ার আগে ১ মিলিয়ন বিটকয়েন মাইনিং করেছিলেন বলে অনুমান করা হয়।
- ১৯,০০০ ডলার/বিটকয়েনের মূল্যে (ডিসেম্বর/১৭ সালে) তিনি ২০১৭ সালে ১৯ বিলিয়ন ডলারের মালিক ছিলেন।

### ২.২.৩. বাংলাদেশে ক্রিপ্টো-কারেন্সি

বাংলাদেশে কোনো ক্রিপ্টো-কারেন্সি উৎপাদন বা মাইনিং করা হয় না, তবে এর ক্রয়-বিক্রয় সংক্রান্ত কার্যক্রম রয়েছে।

ক্রিপ্টো-কারেন্সি সম্পর্কে বাংলাদেশ ব্যাংকের (বাংলাদেশ কেন্দ্রীয় ব্যাংক) নির্দেশনা : বাংলাদেশ ব্যাংক ১৫ সেপ্টেম্বর ২০১৪-এ একটি বিজ্ঞপ্তি জারি করে যার মধ্যে রয়েছে—

- এটা লক্ষ্য করা গেছে যে কিছু লোক বিটকয়েন ক্রয়-বিক্রয়ের সঙ্গে জড়িত।
- এই ধরনের লেনদেন বৈদেশিক মুদ্রা নিয়ন্ত্রণ বিধি, ১৯৪৭ লঙ্ঘন হতে পারে।
- বিটকয়েন লিগ্যাল টেন্ডার (legal tender) নয় এবং বাংলাদেশ ব্যাংক দ্বারা স্বীকৃত নয়।
- এইভাবে বিটকয়েনের সঙ্গে লেনদেনে নিযুক্ত ব্যক্তিরা আর্থিক ক্ষতির সম্মুখীন হতে পারে।
- আর্থিক ক্ষতি ও আইনানুগ ব্যবস্থা এড়াতে সবাইকে বিটকয়েন লেনদেন করা বা লেনদেনে সাহায্য করা থেকে বিরত থাকার জন্য অনুরোধ করা হচ্ছে।

আবার ২৪ ডিসেম্বর, ২০১৭ এ বাংলাদেশ ব্যাংক আকোউ বিজ্ঞপ্তি জারি করে যার মধ্যে রয়েছে—

সংবাদ মাধ্যমে জানা গেছে, বাংলাদেশে বিভিন্ন ক্রিপ্টো-কারেন্সি যেমন বিটকয়েন, ইথেরিয়াম, রিপল, লাইটকয়েন ইত্যাদি লেনদেন হচ্ছে।

- এই ক্রিপ্টো-মুদ্রাগুলো লিগ্যাল টেন্ডার (legal tender) নয়, তাই তাদের বিরুদ্ধে কোনো আর্থিক দাবি প্রতিষ্ঠিত করা যাবে না।
- এগুলো কেন্দ্রীয় ব্যাংক বা বাংলাদেশ সরকার কর্তৃক স্বীকৃত নয়।
- অজানা ব্যক্তির সঙ্গে অনলাইনে লেনদেন করা মানি লন্ডারিং বা সন্ত্রাসী অর্থায়নের সঙ্গে যুক্ত হওয়ার ঝুঁকি রয়েছে।
- দেশের সকল নাগরিককে ক্রিপ্টো-কারেন্সির সঙ্গে লেনদেন এড়াতে অনুরোধ করা হচ্ছে।

### ২.২.৪. লিগ্যাল টেন্ডার (legal tender) কী?

একটি কেন্দ্রীয় ব্যাংক দ্বারা জারি করা মুদ্রার পরিমাণ প্রধানত স্বর্ণ এবং/অথবা সরকরি নিরাপত্তা (যেমন দীর্ঘমেয়াদি বন্ড এবং ট্রেজারি বিল) যা কর, শুল্ক এবং অন্যান্য রাজস্বের মতো সরকারি আয়ের বিপরীতে ইস্যু করা হয়, এরুপ কিছু দ্বারা সমর্থিত (backed) থাকে।

ভেনেজুয়েলা পেট্রো নামে একটি ক্রিপ্টো-মুদ্রা জারি করেছে যা তার তেল রিজার্ভ দ্বারা সমর্থিত।

### ২.২.৫. ক্রিপ্টো-কারেন্সির বর্তমান অবস্থা

- বিটকয়েন, ইথার, লাইট-কয়েন, মনেরো, ড্যাশ, পঞ্জি-কয়েন, জেড ক্যাশ, কার্বন, টিথার, পেট্রো-এর মতো অনেক ক্রিপ্টো-কারেন্সি রয়েছে।
- এগুলো ক্যাশের একটি ইলেকট্রনিক সংস্করণ, কেন্দ্রীয় ব্যাংক দ্বারা নিয়ন্ত্রিত নয়।

- কোনো ভৌগোলিক সীমানা নেই।
- ব্যবহারকারীদের কোন KYC -এর প্রয়োজন হয় না।
- কোনো নির্দিষ্ট কর্তৃপক্ষ নেই। এভাবে কোনো ভোক্তা সুরক্ষা এবং কোন AML/CFT প্রতিবেদন নেই।
- মূল্য কোনো সম্পদ দ্বারা সমর্থিত নয়।

তাই ক্রিপ্টো-কারেন্সি সত্যিকারে কারেন্সি হতে ব্যর্থ হয়েছে। এটি প্রায়শ এইসব কাজের জন্য ব্যবহৃত হয়—

—ড্রাগ এবং অন্যান্য অবৈধ পণ্য কেনা।

—মুক্তিপণ প্রদান, মানব পাচারের অর্থ প্রদান।

—সংগঠিত সন্ত্রাসী গোষ্ঠীকে অর্থ প্রদান।

### ২.২.৬. ক্রিপ্টো-কারেন্সি কীভাবে কাজ করে?

ক্রিপ্টো-মুদ্রার সঙ্গে জড়িত পক্ষগুলো হলো :

১. মাইনারস্ (Miners)
২. ব্যবহারকারী (Users)
৩. অনলাইন ওয়ালেট প্রদানকারী (Online Wallet Providers)
৪. বিনিময় কোম্পানি (Exchange Companies)

i) মাইনিং (Mining)- মাইনিং হলো ক্রিপ্টো-কারেন্সি উৎপাদনের প্রক্রিয়া।

- মাইনাররা বিটকয়েন তৈরি করে, রেকর্ড করে এবং ইন্ট্রিগ্রিটি নিশ্চিত করে।
- বিনিময়ে, তারা উৎপন্ন বিটকয়েনের মালিক হয়ে যায় এবং অল্প পরিমাণ ফিও পায়।
- নেটওয়ার্কটি এমনভাবে ডিজাইন করা হয়েছে যে কোনো প্রতিযোগিতায়, মাইনিংয়ে ১ বিটকয়েন তৈরি করতে ১০ মিনিট সময় লাগবে এবং সর্বোচ্চ ২১মিলিয়ন বিটকয়েন তৈরি করা যেতে পারে (২১৪০ সালে সর্বোচ্চ উৎপাদন শেষ হবে)।
- বিটফার্মস হলো মন্ট্রিলের একটি মাইনিং কোম্পানি, যা মাইনিং করতে বিপুল বিদ্যুৎ খরচ করে (অস্ট্রিয়ার মতো দেশের মোট খরচের সমান)।
- কোম্পানিটি একটি বিশাল ডেটা সেন্টার নির্মাণ করেছে এবং বড় বড় কম্পিউটার ও সরঞ্জাম স্থাপনে বিপুল পরিমাণ অর্থ বিনিয়োগ করেছে।
- কোম্পানিটি ২০১৭ সালে ৪.৫ বিলিয়ন ডলার আয় করেছে।

উৎপাদন প্রক্রিয়াকে বোধগম্য করতে, উদাহরণ হিসাবে ধরা যায় যে এই বিশ্বে ক্রিপ্টো-মুদ্রা উৎপাদনে নিযুক্ত শুধু একজন মাইনার ও একটি কম্পিউটার (তাই কোনো প্রতিযোগিতা নেই!)। ধরুন, কম্পিউটারের গতি ২ GHz এবং আমরা জানি ১টি বিটকয়েন তৈরিতে ১০ মিনিট সময় লাগে। যেহেতু কোনো প্রতিযোগিতা নেই, মাইনার প্রতি ১০ মিনিটে ১টি বিটকয়েন তৈরি করবে।

এখন বিশ্বে, ধরুন দুটি কম্পিউটার/মাইনার আছে এবং মনে করুন, কম্পিউটার—১ এর গতি ২ GHz এবং কম্পিউটার-২ এর গতি ১০ GHz। সুতরাং কম্পিউটার—১-এর তুলনায় কম্পিউটার-২ এর বিটকয়েন (লটারির মতো) জেতার/উৎপাদনের সম্ভাবনা ৫ গুণ বেশি। সুতরাং ১২০ মিনিটে, ১২টি বিটকয়েন তৈরি হবে—২টি মাইনার-১ দ্বারা এবং ১০টি মাইনার-২ দ্বারা।

বিশ্বে মাইনারের সংখ্যা বাড়লে, জেতার সুযোগ কমে যাবে। যাহোক, যদি একটি কম্পিউটারের জটিল অ্যালগরিদম গণনার গতি বেশি হয়, সেটির জয়ের উচ্চ সম্ভাবনা রয়েছে।

**ii) ক্রিপ্টো-কারেন্সি ব্যবহারকারী (End-users of Crypto-currency)**

১. গ্রাহকদের (এন্ড ইউজার) তাদের কম্পিউটারে ব্লকচেইন সফ্টওয়্যারের একটি সম্পূর্ণ কপি ডাউনলোড করতে হবে এবং লেনদেন প্রক্রিয়াগুলো নিজেরাই সংরক্ষণ করতে হবে।
২. তাদের সংশ্লিষ্ট প্রাইভেট কী একটি সুরক্ষিত জায়গায় রাখতে হবে (যথাযথ ব্যাকআপসহ পেনড্রাইভ স্টিকে বা কম্পিউটারের হার্ডডিস্কে হারিয়ে গেলে, কোনো লেনদেন সম্ভব নয় এবং বিটকয়েনও হারিয়ে যাবে)।
৩. একটি বিটকয়েন খরচ করার জন্য, মালিককে সংশ্লিষ্ট প্রাইভেট কী জানতে হবে এবং লেনদেনে ডিজিটালি স্বাক্ষর করতে হবে। নেটওয়ার্ক এটির সংশ্লিষ্ট পাবলিক কী ব্যবহার করে স্বাক্ষর যাচাই করে।

কিন্তু বিধি # ১ ও ২ বজায় রাখা ব্যয়বহুল এবং এন্ড ইউজারের জন্য অসুবিধাজনক। এটি এড়াতে, এন্ড ইউজারগণ অনলাইন ওয়ালেট প্রদানকারীদের সাহায্য নেয়।

**iii) অনলাইন ওয়ালেট প্রদানকারী (Online Wallet Providers)**

- অনলাইন ওয়ালেট প্রদানকারী একটি প্রযুক্তি সংস্থা, যা তাদের নিজ নিজ গ্রাহকদের গোপনীয় তথ্য ও লেনদেনের ইতিহাস সংরক্ষণ করে। ফলে

গ্রাহকদের ব্লক চেইন সফ্টওয়্যারটির সম্পূর্ণ অনুলিপি ডাউনলোড করতে হয় না এবং নিজেদের ডেটা সংরক্ষণ করতে হয় না।

- তহবিল অ্যাক্সেস করতে ব্যবহারকারীর গোপনীয় তথ্য প্রদানকারীদের (Providers) কাছে সংরক্ষণ করা হয়, ফলে এ ধরনের ব্যবহারকারীদের অবশ্যই প্রদানকারীদের (Providers) ওপর পূর্ণ আস্থা থাকতে হবে।
- একটি দূষিত (malicious) প্রদানকারী (Provider) বা প্রদানকারীর সার্ভারে নিরাপত্তার ঘাটতির কারনে গ্রাহকের বিটকয়েন চুরি হতে পারে।

### iv) বিনিময় কোম্পানি (Exchange Company)

এক্সচেঞ্জ কোম্পানিগুলো হলো এজেন্ট যেখানে বিটকয়েন প্রচলিত মুদ্রার বিনিময়ে লেনদেন করা হয় (যেমন এমএফএস কোম্পানিগুলোর এজেন্ট)। আমাদের দেশে প্রাতিষ্ঠানিক নয়, কিন্তু ব্যক্তিগত এজেন্ট বিদ্যমান।

### ২.২.৭. সমাধান কী?

এটা খুবই কঠিন—

১. ক্রিপ্টো-মুদ্রার ব্যবহার শনাক্ত, তদন্ত, বিচার এবং প্রতিরোধ করা।
২. ক্রিপ্টো সম্পদ জব্দ করা।
৩. তহবিলের গতিবিধি অনুসরণ করা।
৪. কাউকে STR ফাইল তৈরিতে বাধ্য করা।

কারণ জড়িত সব ব্যক্তি/পক্ষ বেনামি এবং শনাক্তযোগ্য নয়।

যদি এটি নিয়ন্ত্রন করা না যায়, তাহলে এটি বৈধ ওয়ালেট এবং প্রকৃত মুদ্রাকে হত্যা করবে। ইতোমধ্যে, যেমন প্রতিবেদন করা হয়েছে, ভার্চুয়াল ক্রেডিট কার্ড ও ডেবিট কার্ড ইস্যু করা এবং ভার্চুয়াল অ্যাসেট এটিএম ইনস্টল করা শুরু হয়েছে।

তাই ক্রিপ্টো-কারেন্সির ধারণাটি গ্রহণ করা এবং সংশ্লিষ্ট দেশের কেন্দ্রীয় ব্যাংকগুলো দ্বারা ডিজিটাল মুদ্রা চালু করা বুদ্ধিমানের কাজ হবে। এটি অবৈধ ভার্চুয়াল সম্পদকে ধ্বংস করবে এবং দেশ থেকে নগদ অর্থ সরিয়ে ক্যাশলেস সমাজ গঠনে সাহায্য করবে। আইএমএফ প্রধান ক্রিস্টিন লাগার্ড সিঙ্গাপুরে একটি সম্মেলনে তার সাম্প্রতিক বক্তৃতায় বলেছেন (রেফারেন্স : বিবিসি (১৪ নভেম্বর ২০১৮)) 'কেন্দ্রীয় ব্যাংক ডিজিটাল মানি ইস্যু করতে পারে'।

তিনি আরও বলেন—

- আমি বিশ্বাস করি আমাদের ডিজিটাল মুদ্রা চালু করার সম্ভাবনা বিবেচনা করা উচিত।
- ডিজিটাল অর্থনীতিতে অর্থ সরবরাহে রাষ্ট্রের ভূমিকা থাকতে পারে।
- সুবিধাগুলো স্পষ্ট। আপনার পেমেন্ট তৎক্ষণাৎ, নিরাপদ, সস্তা ও অর্ধ-বেনামি হবে।
- কানাডা, চীন, সুইডেন ও উরুগুয়ের কেন্দ্রীয় ব্যাংকগুলো ডিজিটাল কারেন্সির প্রস্তাবসমূহ গুরুত্ব সহকারে বিবেচনা করছে।
- একটি কেন্দ্রীয় ব্যাংক দ্বারা জারি করা একটি ভার্চুয়াল মুদ্রা ক্যাশের মতোন রাষ্ট্রের দায় হবে—একটি প্রাইভেট ফার্মের নয়।
- এটি লেনদেনগুলোকে নিরাপদ এবং আরও সহজ করে, ফলে সস্তা হবে।

### ২.২.৮. জাতীয় ডিজিটাল মুদ্রার (এনডিসি) পরিচিতি : (Introduction of National Digital Currency (NDC))

i) বিটকয়েনে, মাইনার অপরিচিত এবং তারা ব্যবসায়িক লক্ষ্য হিসাবে বিশাল তথ্য কেন্দ্র স্থাপন করে। ন্যাশনাল ডিজিটাল মুদ্রার ক্ষেত্রে কেন্দ্রীয় ব্যাংক হবে একমাত্র মাইনার।

ii) বিটকয়েনে, ইউজারগণ অপরিচিত থাকে, অন্যদিকে জাতীয় ডিজিটাল মুদ্রায় ইউজাররা নির্বাচন কমিশন ডাটাবেস থেকে ই-কেওয়াইসি যাচাইকরণের মাধ্যমে ব্যাংক কর্তৃক নিবন্ধিত হবে।

iii) বিটকয়েনের অনলাইন ওয়ালেট প্রদানকারীরা অপরিচিত পক্ষ (কোন কর্তৃপক্ষ দ্বারা নিয়ন্ত্রিত নয়) পক্ষান্তরে ন্যাশনাল ডিজিটাল কারেন্সিতে কমার্শিয়াল ব্যাংকগুলো অনলাইন ওয়ালেট প্রদানকারী হিসেবে কাজ করবে।

iv) বিটকয়েনের ক্ষেত্রে, এক্সচেঞ্জ কোম্পানিগুলো লুকানো থাকে এবং এগুলো কোনও কর্তৃপক্ষের দ্বারা নিয়ন্ত্রিত নয়। অন্যদিকে জাতীয় ডিজিটাল মুদ্রার ক্ষেত্রে, যদি টাকার সঙ্গে এনডিসি বিনিময় করতে না হয়, তখন কোন এক্সচেঞ্জ কোম্পানির প্রয়োজন হয় না, আর বিনিময়ের প্রয়োজন হলে, ব্যাংকের শাখা, মানি এক্সচেঞ্জ এবং/অথবা এমএফএস বা এজেন্ট ব্যাংকিং আউটলেটকে টাকাকে এনডিসি-তে বা এনডিসিকে টাকাতে রূপান্তর করার জন্য নিয়োজিত করা যেতে পারে।

## ৩. কৃত্রিম বুদ্ধিমত্তা (Artificial Intelligence)

কৃত্রিম বুদ্ধিমত্তা (AI) হলো এমন বুদ্ধিমত্তা, যা মেশিন ব্যবহার করে যৌক্তিকতার পরিপ্রেক্ষিতে এবং যুক্তিসঙ্গতভাবে শিক্ষা এবং সমস্যা সমাধানের কৌশল প্রদান করে। AI গবেষণাকে বুদ্ধিমান এজেন্টের অধ্যয়নের ক্ষেত্র হিসাবে সংজ্ঞায়িত করা হয়েছে, যা এমন কোনো পদ্ধতিকে বোঝায় যা তার পরিবেশকে সম্ভাব্য করে এবং এমন পদক্ষেপ নেয়, যা তার লক্ষ্য অর্জনের সম্ভাবনাকে সর্বাধিক করে তোলে। এর

মধ্যে রয়েছে উন্নত ওয়েব সার্চ ইঞ্জিন, মানুষের কথা বোঝা, স্বয়ংক্রিয়ভাবে গাড়ি চালানো, স্বয়ংক্রিয় সিদ্ধান্ত গ্রহণ ও কৌশলগত গেম পদ্ধতিতে সর্বোচ্চ পর্যায়ে প্রতিযোগিতা করা।

আর্থিক শিল্প যেখানে প্রচুর পরিমাণে ডেটা সৃষ্টি করে সেখানে বিগ ডেটা (big data) পাওয়া যায়। তথ্য সংগ্রহ, গঠন ও সংরক্ষণের জন্য ব্যাংকিং শিল্পের একটি শক্তিশালী টুলের প্রয়োজন। অনেক ব্যাংকিং ও আর্থিক প্রতিষ্ঠান কৃত্রিম বুদ্ধিমত্তা প্রযুক্তি ব্যবহার করছে যেমন best integrated database তৈরি ও ব্যবহার করা, গ্রাহকের এক্সপেরিয়েন্স উন্নতি করা, ঝুঁকি ব্যবস্থাপনা উন্নত করা, তথ্য নিরাপত্তার উন্নতি করা, রেগুলেটরি কমপ্লায়েন্স বৃদ্ধি করা, ইত্যাদি।

আমরা ব্যাংকিং-এ কৃত্রিম বুদ্ধিমত্তার প্রভাবকে দুটি দৃষ্টিকোণ থেকে বিবেচনা করতে পারি।

**গ্রাহকদের দৃষ্টিকোণ থেকে**

১. কৃত্রিম বুদ্ধিমত্তা ভার্চুয়াল সাহায্যকারীর মাধ্যমে অ্যাকাউন্ট খোলাতে সহায়তা করে।
২. অ্যাকাউন্ট শনাক্তকরণ এবং অর্থ লেনদেনের জন্য বায়োমেট্রিক্স (মুখ/আইরিস/ভয়েস/আঙুলের ছাপ শনাক্তকরণ) এর ব্যবহার।
৩. প্রতিটি গ্রাহককে একটি ব্যক্তিগত এক্সপেরিয়েন্স প্রদান করা।
৪. AI -সক্ষম সুরক্ষিত ব্যাংকিং সুবিধা প্রদান।

**ব্যাংকের দৃষ্টিকোণ থেকে**

১. একাধিক সংস্থান থেকে স্বতন্ত্রভাবে গ্রাহক শনাক্তকরণ।
২. প্রাসঙ্গিক ডেটার উপর ভিত্তি করে মেশিন লার্নিং অ্যালগরিদম ব্যবহার করে গ্রাহকদের জন্য ঋণের যোগ্যতার বিষয়ে সিদ্ধান্ত নেওয়া এবং একটি লোনের লিমিট বের করা।
৩. জালিয়াতি শনাক্তকরণ ও সন্দেহজনক আচরণ শনাক্তকরণ।
৪. সবচেয়ে বেশি ব্যবহৃত সেবাগুলো খুঁজে বের করা এবং সেই অনুযায়ী সেবা প্রদান করা।
৫. ব্যবস্থাপনা ও ব্যাংক কর্মচারীদের সেবার মানগুলোর জন্য মনিটরিং টুলস্ প্রদান করা।
৬. প্রচুর পরিমাণে রো (raw) ব্যাংকিং ডেটা থেকে সংক্ষিপ্ত ইনসাইট (insite) তৈরি করা, যা ভবিষ্যতে ব্যাংকিং কৌশল গঠনে সাহায্য করতে পারে।
৭. গ্রাহকদের ডেটার ওপর ভিত্তি করে গ্রাহকদের জন্য নতুন নতুন অফার/প্যাকেজ/সার্ভিস তৈরি করা।
৮. গ্রাহকদের জন্য ভৌগোলিক, এবং আর্থ-সামাজিক ডেটা।
৯. প্রতিযোগীদের বিশ্লেষণ করা ও প্রতিযোগিতাপূর্ণ বাজারে অন্যদের চেয়ে এগিয়ে থাকার কৌশল নির্ণয় করা।
১০. লাভ করার জন্য প্রতিশ্রুতিবদ্ধ বিনিয়োগ সেক্টর (Promising investment sector) খুঁজে বের করা।
১১. মূল্যস্ফীতি ও মুদ্রা সংকটসহ ব্যাংকিং সংকটের পূর্বাভাস পেতে গভীর শিক্ষার মডেলগুলো (deep learning models) বেশ কার্যকর হতে পারে।

## ৪. ভবিষ্যত প্রযুক্তিভিত্তিক ব্যাংকিং (Future Technology-based banking)

### ৪.১ ভার্চুয়াল/ডিজিটাল ব্যাংকিং (Virtual/Digital Banking)

ভার্চুয়াল/ডিজিটাল ব্যাংকিং বলতে কোনো গ্রাহক ব্যাংক শাখায় ফিজিক্যাল উপস্থিতি ছাড়াই ব্যাংকিং প্রতিষ্ঠান এবং তাদের কার্যাবলি অনলাইনে অ্যাক্সেস করাকে বোঝায়। ব্যাংকিংয়ে প্রযুক্তির ব্যাপক ব্যবহারের মাধ্যমে এটা সম্ভব।

বাংলাদেশের অনেক ব্যাংক ইতিমধ্যে ভার্চুয়াল/ডিজিটাল ব্যাংকিং সেবা চালু করেছে এবং সবচেয়ে জনপ্রিয় সেবাগুলো হলো ইন্টারনেট ব্যাংকিং, ই-কমার্স সলিউশন, মোবাইল অ্যাপস। এটিএম/সিআরএম, এমএফএস ও এজেন্ট ব্যাংকিংয়ের মতো অন্যান্য পরিষেবা গ্রহণের জন্য গ্রাহকদের বুথ, এজেন্ট পয়েন্ট ইত্যাদির মতো স্থানে যেতে হয়।

ভার্চুয়াল/ডিজিটাল ব্যাংকিং সেবায় মানুষের প্রধান উদ্বেগের মধ্যে একটি হলো নিরাপত্তা। স্ক্যামার ও হ্যাকারদের কারণে ইন্টারনেটে ব্যাংকিং অনেকের কাছে ভীতিকর হতে পারে, তাই ভার্চুয়াল ব্যাংক তাদের প্ল্যাটফর্মগুলো নিরাপদ ও আর্থিক ক্রিয়াকলাপের জন্য উপযুক্ত কিনা তা নিশ্চিত করতে অতিরিক্ত সতর্কতা অবলম্বন করবে।

অন্যদিকে, ভার্চুয়াল/ডিজিটাল ব্যাংক হলো এমন একটি ব্যাংক—যার কোনো ফিজিক্যাল উপস্থিতি নেই। গ্রাহকরা অনলাইনে একটি ভার্চুয়াল ব্যাংকে অ্যাকাউন্ট খোলে এবং কার্যত সমস্ত লেনদেন অনলাইনে সম্পাদন করে। গ্রাহকদের কোনো সহায়তার প্রয়োজন হলে ভার্চুয়াল ব্যাংকের কল সেন্টার তাদের সহায়তা দেবে।

### ৪.২ ক্লাউড কম্পিউটিং (Cloud Computing)

ক্লাউড কম্পিউটিং হলো সার্ভার, স্টোরেজ, ডাটাবেস, নেটওয়ার্কিং, সফ্টওয়্যার, এনালাইটিকস্ ও বুদ্ধিমত্তাসহ কম্পিউটিং পরিষেবা ইন্টারনেট (বা ক্লাউড) এর মাধ্যমে সরবরাহ করা। ফিজিক্যাল ডেটা সেন্টার ও সার্ভার কেনা, মালিকানা গ্রহণ ও রক্ষণাবেক্ষণের পরিবর্তে, আমরা যখন প্রয়োজন তখন এবং Pay-as-you-go ভিত্তিতে প্রযুক্তিগত সেবাসমুহ অ্যাক্সেস করতে পারি।

ক্লাউড কম্পিউটিং ব্যাংকিং সেক্টরের জন্য সবচেয়ে আকর্ষণীয় ও প্রতিশ্রুতিশীল প্রযুক্তিগুলোর মধ্যে একটি। তবে বিদ্যমান নিয়মানুসারে, গ্রাহকের তথ্য দেশের বাইরে অবস্থান করতে পারবে না এবং ব্যাংকগুলো ব্যাংকিং সেবা, বিশেষ করে কোর ব্যাংকিং সলিউশনের জন্য ক্লাউড ব্যবহার করতে পারবে না। তবে ব্যাংকগুলো এইচআর, ইনভেন্টরি ও ইমেইলের মতো বিবিধ পরিষেবাগুলোর জন্য ব্যাপকভাবে ক্লাউড কম্পিউটিং ব্যবহার করেছে।

### ক্লাউড কম্পিউটিং এর ধরন

- Business Process as-a-Service (BPaaS)
- Intrastructure as-a-Service (IaaS)
- Platforms as-a-Service (PaaS)
- Software as-a-Service (SaaS)

যদিও ক্লাউড ব্যাংকিংয়ের সুবিধা হলো বর্ধিত তৎপরতা ও উদ্ভাবন, কম রক্ষণাবেক্ষণ ব্যয়, আইটি জটিলতা হ্রাস করা এবং নিরাপত্তা বৃদ্ধি করা; এর চ্যালেঞ্জগুলো হচ্ছে—

- স্থানীয় রেগুলেটরের গাইডলাইন ও ক্লাউড ব্যাংকিংয়ের কমপ্লায়েন্সের নিয়মগুলোর মধ্যে দ্বন্দ্ব।
- নিরাপত্তা ও গোপনীয়তার হুমকি, যেমন, তথ্য আপস করা।
- বিদ্যমান পদ্ধতি থেকে ক্লাউডে তথ্য স্থানান্তরের ঝুঁকি, যেমন বিপুল পরিমাণ তথ্য, অযোগ্য প্রযুক্তিবিদ, লেগেছি (Legacy) সফ্টওয়্যার, ইত্যাদি।
- ক্লাউডে মাইগ্রেশনের কাজটি আউটসোর্সিংয়ের কারণে ইউজার ডেটা বিপন্ন হওয়ার ঝুঁকি।
- মানব ত্রুটি এবং অযোগ্যতা, বিশেষ করে কোডিং, মাইগ্রেশন, রক্ষণাবেক্ষণ ইত্যাদির ক্ষেত্রে।
- নিরবচ্ছিন্ন আন্তঃসীমান্ত ইন্টারনেট এবং উচ্চ ব্যান্ডউইথ।

### ৪.৩ ইন্টারনেট অফ থিংস (IOT)

IOT ভৌত বস্তুর 'things' (মোবাইল ফোন, বৈদ্যুতিক যন্ত্রপাতি, বারকোড সেন্সর, ট্র্যাফিক লাইট, ইত্যাদি) যাতে সেন্সর, সফ্টওয়্যার এবং অন্যান্য প্রযুক্তিগত মাইক্রোপ্রসেসর সংযুক্ত থাকে, এবং যাহা ইন্টারনেটের মাধ্যমে অন্যান্য ডিভাইস ও পদ্ধতির সঙ্গে তথ্য আদান-প্রদান করতে পারে, এমন জিনিসের নেটওয়ার্ককে বোঝায়।

### কীভাবে IOT কাজ করে

—ইন্টারনেট—সংযুক্ত ডিভাইসগুলো তথ্য সংগ্রহ করে।
—সংগৃহীত তথ্য ডিভাইসগুলো থেকে একটি সংগ্রহস্থলে (gathering print) প্রেরণ করা হয়, যেমন—ডেটা সেন্টার, ক্লাউড ইত্যাদি।
—তথ্য প্রক্রিয়াকরণ ও বিশ্লেষণ করে।
অনুমতি দেওয়া হলে গ্রাহকরা এই তথ্যাগুলো অ্যাক্সেস করতে পারেন এবং IOT—সক্ষম ডিভাইসগুলোতে রিমোট কমান্ড প্রয়োগ করা, অনলাইনে এমআইএস প্রতিবেদন পাওয়া এবং কাস্টমাইজড বিশ্লেষণ সম্পাদন করার মতো কিছু ক্রিয়াকলাপ সম্পাদন করতে পারেন। IOT গ্রাহকদের ও ব্যাংকারদের ব্যাংকিং এক্সপেরিয়েন্স বাড়াতেও ব্যবহার করা যেতে পারে।

### ৪.৪ মেশিন লার্নিং (Machine Learning)

যখন একটি কম্পিউটার হাজার হাজার বিস্তৃত পরিসংখ্যানগত (Statistical) ও গাণিতিক (Mathmetical) মডেলের সাহায্যে পুরাতন ডেটা এবং তথ্য ব্যবহার করে নিজে নিজে শেখার জন্য কনফিগার করা হয়, তখন একে মেশিন লার্নিং বলে। ক্রেডিট স্কোরিং ও উপযুক্ত বিনিয়োগ পরামর্শের জন্য রোবো-উপদেষ্টা (Robo-advisor), দক্ষ গ্রাহক সেবার জন্য চ্যাটবট, ইত্যাদি হলো ইদানীং ব্যবহৃত সবচেয়ে কমন মেশিন লার্নিং-ভিত্তিক অ্যাপ্লিকেশন।

জালিয়াতি শনাক্তকরণ, ঝুঁকি ব্যবস্থাপনা, গ্রাহকের আচরণ বিশ্লেষণ, ক্রয়ের ধরণ এবং ব্যাংকের অন্যান্য অনেক কাজ, মেশিন লার্নিং ব্যবহার করে উন্নত করা যেতে পারে। উদাহরণস্বরূপ, যদি একটি ক্রেডিট কার্ড এখন বাংলাদেশে ব্যবহার করা হয় এবং তারপর আধা ঘণ্টার মধ্যে এটি যদি মার্কিন যুক্তরাষ্ট্রে ব্যবহার করা হয়, তাহলে সিস্টেম এটি একটি প্রতারণামূলক লেনদেন হিসাবে শনাক্ত করবে, কারণ কোনো গ্রাহক আধা ঘণ্টার মধ্যে বাংলাদেশ থেকে মার্কিন যুক্তরাষ্ট্রে যেতে পারবে না। অন্যান্য ব্যবহারের ক্ষেত্রে হতে পারে কার্যাবলি স্বয়ংক্রিয় করা,

জালিয়াতি হওয়ার আগেই তা চিহ্নিত করা, আরও দ্রুত ও নির্ভুলভাবে ঋণ প্রক্রিয়া করা এবং কমপ্লায়েন্স চেকের কার্যকারিতা বাড়ানো।

ব্যাংকের জন্য মেশিন লার্নিং প্রয়োগ করার সুবিধা হলো পরিচালনা ব্যয় কমানো এবং আয় বাড়ানো। মেশিন লার্নিং একটি কোম্পানিকে তার প্রতিযোগীদের চেয়ে বেশি ভালো করার ক্ষমতা বৃদ্ধি করবে। এরপরও, লোকেরা কীভাবে তাদের অর্থ ব্যয় করে তা আরও ভালোভাবে বোঝার মাধ্যমে, মেশিন লার্নিং অ্যালগরিদমগুলো অফার, ডিসকাউন্ট ও প্রোডাক্ট প্রস্তাব করতে পারে, যা গ্রাহকরা কিনতে বা যাতে আরও বিনিয়োগ করতে আগ্রহী হয়।

### ৪.৫ ডেটা মাইনিং (Data Mining)

ডেটা ব্যবস্থাপনা প্রযুক্তির সঙ্গে সামঞ্জস্য রেখে সাম্প্রতিক অগ্রগতির মধ্যে একটি হলো ডেটা মাইনিং ও জ্ঞান আবিষ্কার (knowledge discover)। ডেটা মাইনিং হচ্ছে মেশিন লার্নি, পরিসংখ্যান ও ডাটাবেস সিস্টেমের সংযোগস্থলে জড়িত বৃহৎ ডেটাসেটের প্যার্টান বের করা ও আবিষ্কার করার প্রক্রিয়া। ডেটা আকারে ও মাত্রায় বৃদ্ধি পেয়েছে। এসত্ত্বেও এটি প্রায়শই গ্রাহককে জানার ও সেরা বিকল্পগুলো তৈরির একটি টুল হিসাবে ব্যবহৃত হয়।

গুরুত্বপূর্ণ ব্যবসায়িক উদ্বেগগুলোকে (important business concerns) মোকাবেলায় বিশাল তথ্য ভান্ডার থেকে দরকারি তথ্য সন্ধান করার কৌশলকে ডেটা মাইনিং বলে। তথ্যের এই পর্বত, যা প্রতিদিনই সংরক্ষণ করা হচ্ছে তা প্রতিষ্ঠানের সবচেয়ে মূল্যবান সম্পদে পরিণত হচ্ছে। বিপণন, ঋণ ঝুঁকি ব্যবস্থাপনা, অর্থ পাচার সনাক্তকরণ, তারল্য ব্যবস্থাপনা, ইনভেন্টমেন্ট ব্যাংকিং ও সময়মতো প্রতারণামূলক লেনদেন শনাক্তকরণসহ বিভিন্ন ক্ষেত্রে ব্যাংকগুলোর দ্বারা ডেটা মাইনিংয়ের ব্যবহারের প্রচুর সম্ভাবনা রয়েছে। এটি ব্যাংক এর লেনদেনের ধরনগুলো বিশ্লেষণ করে এর লাভের ওপর প্রভাব ফেলার আগেই জালিয়াতি শনাক্ত করতে পারে। ডেটা মাইনিং অত্যন্ত কাঙ্ক্ষিত গুণাবলি অর্জনে কার্যকর হতে পারে।

### ৪.৬. তথ্য সংরক্ষণাগার (Data warehouse)

ডেটা ওয়ারহাউজিং প্রতিবেদন ও ডেটা বিশ্লেষণের জন্য ব্যবহৃত একটি পদ্ধতি এবং ব্যবসায়িক বুদ্ধিমত্তার একটি মূল উপাদান হিসাবে বিবেচিত হয়। এটি এক বা একাধিক উৎস থেকে সমন্বিত তথ্যের এক ধরনের কেন্দ্রীয় সংগ্রহস্থল। উদাহরণস্বরূপ, একটি ব্যাংকের বিভিন্ন ডেটাবেস থাকতে পারে যেমন কোর ব্যাংকিং ডেটা, রিটেইল, ঋণ তথ্য, এসএমই ঋণ দেওয়ার তথ্য, ক্রেডিট কার্ড তথ্য, এমএফএস তথ্য, ই-কমার্স তথ্য ও এজেন্ট ব্যাংকিং তথ্য। একটি তথ্য সংরক্ষণাগার সমস্ত তথ্যকে একত্রিত করে এবং গ্রাহক নম্বর, মোবাইল নম্বর বা এনআইডি নম্বরের মতো কিছু মূল শনাক্তকারী (key identities) ব্যবহার করে সেগুলোকে সাজায়। পদ্ধতি দ্বারা কিছু অত্যন্ত গুরুত্বপূর্ণ সিদ্ধান্ত নেওয়া হয় এবং প্রতিবেদন হিসাবে ব্যাংকিং কর্মকর্তাদের কাছে জমা দেওয়া হয়।

বিশ্লেষণ বা প্রতিবেদনের সাহায্যে, ব্যাংকগুলো তাদের গ্রাহকদেরকে ভাগ করে ব্যাংকের মুনাফা বাড়াতে ও নতুন গ্রাহকদের আকৃষ্ট করতে পারে। ব্যাংকগুলোর জন্য, তথ্য সংরক্ষণ পরিষেবাগুলো গ্রাহকের অনেক প্রশ্ন বা জিজ্ঞাসার ফল।

তাই সংক্ষেপে, তথ্য সংরক্ষণাগার হলো ব্যাংকগুলো দ্বারা তথ্য মোকাবেলা ও পরিচালনায় ব্যবহৃত টুলস্ যা তাদের গ্রাহকের চাহিদাগুলো আরও ভালোভাবে বুঝতে এবং আরও ঘনিষ্ঠভাবে দেখতে সাহায্য করতে পারে। যখন একটি প্রতিষ্ঠান উপযুক্ত ডেটা ও এনালিস্ট ব্যবহার করে, তখন এটি সম্প্রসারণ ও হ্রাসের (expansion and depletion) মধ্যে পার্থক্য করতে পারে। এই জ্ঞান অর্জনে কার্যকর তথ্য ব্যবস্থাপনা ও বিশ্লেষণ অপরিহার্য এবং এটি একটি ডেটা ওয়ারহাউজ সলিউশন ব্যবহার করে অর্জন করা যেতে পারে।

বাণিজ্যিকভাবে সহজলভ্য তথ্য সংরক্ষণকরণ সমাধানগুলোর মধ্যে কয়েকটি হলো টেরাডাটা (Teradata), মাইক্রোসফ্ট অ্যাজুর (Azure), অ্যামাজন রেডশিফ্ট (Redshift), বিগকুয়েরি (BigQuery), এসএপি (SAP) এবং এসএএস (SAS)।

### ৪.৭. সাম্প্রতিক প্রবণতা (Current Trends)

প্রযুক্তিগত উন্নতির সঙ্গে সঙ্গে ব্যাংকিং খাতে ব্যাপক পরিবর্তন ঘটছে। প্রযুক্তি ব্যবসার সমার্থক হয়ে উঠেছে। তাই ব্যাংকিং সেক্টর প্রথাগত ব্যাংকিং থেকে ডিজিটাল ও কৃত্রিম বুদ্ধিমত্তার দিকে এগিয়ে যাচ্ছে। আমরা দীর্ঘকাল ধরে প্রযুক্তির আশীর্বাদ গ্রহণ করেছি, যা কৃত্রিম বুদ্ধিমত্তা, মেশিন লার্নিং, অ্যালগরিদম, ব্লক চেইন, ক্রিপ্টোকারেন্সি, আইওটি, 5G সহ আরও অনেক ভাবে পেয়ে যাচ্ছি।

বর্তমানে ব্যাংকিং সেক্টরে ব্যবহৃত কিছু প্রধান প্রযুক্তি নিচে উল্লেখ করা যেতে পারে—

- নিজের অ্যাকাউন্ট নিজেই খোলা (eKYC)
- ডিজিটাল মানি (ক্রিপ্টোকারেন্সি) যা ক্যাশের ব্যবহার কমিয়ে দেবে।
- যেকোনো ধরনের লেনদেন, তহবিল স্থানান্তর, ব্যালেন্স/বিবৃতি অনুসন্ধান, ই-পেমেন্ট, ই-লোন ইত্যাদির জন্য মোবাইল অ্যাপস।

- কার্ডলেস এটিএম উত্তোলন, সিআরএম ব্যবহার করে টাকা তোলা ও জমা করা।
- QR ও NFC পেমেন্ট।
- IVR (ইন্টারেক্টিভ ভয়েস রেসপন্স) ও ভিডিও ব্যাংকিং।
- ই-কমার্স।
- আঙুলের ছাপ, মুখ শনাক্তকরণ, ভয়েস ব্যাংকিং।

ব্যাংকিং সেক্টরে আসন্ন কৃত্রিম বুদ্ধিমত্তাভিত্তিক প্রযুক্তি

- ব্লকচেন প্রযুক্তির সাহায্যে ভার্চুয়ালাইজেশন ও ক্লাউড-ভিত্তিক ব্যাংকিং।
- ভার্চুয়াল ও বর্ধিত বাস্তবতার (augmented reality) ব্যবহার।
- মেশিন লার্নিং ও ডেটা সায়েন্স ব্যবহার করে ব্যক্তিগতকরণ (Personalisation) ও বুদ্ধিমত্তা পরিষেবা (Intelligence Service) প্রদান।
- BaaS (একটি পরিষেবা হিসাবে ব্যাংকিং) এবং PaaS (একটি পরিষেবা হিসাবে প্ল্যাটফর্ম) ব্যবহার করা।

সঠিকভাবে ডিজিটাল ব্যাংকিংয়ের সুবিধা নিতে নিরাপত্তা একটি প্রধান উদ্বেগ হবে। শক্তিশালী সাইবার নিরাপত্তা, ব্যবহারকারীর পরিচয় (user identity), সুরক্ষিত ডিভাইস ও অবস্থান (location) উচ্চতর অগ্রাধিকার পাবে।

অবশেষে প্রযুক্তির আশীর্বাদে রূপান্তর ঘটবে এবং বাজারে নিজস্ব শেয়ার সুরক্ষিত করতে ব্যাংকগুলোকে ভার্চুয়ালাইজেশন ও ডিজিটাল ব্যাংকিংয়ের ওপর খুব জোরালোভাবে প্রাধান্য দিতে হবে।

# পর্যালোচনামূলক প্রশ্নাবলি

## 1. Multiple Choice Questions (MCQ)

i) Which of the following is not a FinTech for Banks?

a) Credit Card b) ATM c) Q-Management d) Mobile Apps

ii) Which of the following is not a TechFins?

a) Facebook b) Amazon c) Dutch-Bangla Bank d) Grameen Phone

iii) Which of the following is not a party in Crypto-Currency production and processing?

a) Miners b) Central Bank c) Online Wallet Providers d) Exchange Companies

iv) Digital Banking has -----

a) a few branches b) no branches c) a few agents d) huge number of employees

## 2. Fill in the gap(s)

i) The FinTechs are financial companies like -----, ----- and ----- which embad FinTech to make their own products more attractive.

ii) Most well known solutions using FinTech in Bangladesh are ----, ----- and ------

iii) -------refers to any te hnology that ensures companies comply with their regulatory requirements.

iv) ------- invented Bitcoin in -----

v) Amount of currency to be issued by a central bank is backed mainly by ------

vi) ------- is the process of production of crypto-currency.

## সম্ভাব্য প্রশ্নাবলি

1. What is the differences between FinTech and TechFin?
2. Name a few of the FinTech solutions in use in Bangladesh.
3. Is Grameen Phone a TechFin company? Why?
4. Define the following:

   RegTech, Virtual Banking, Cloud computing, Internet ofThings, Machine learning, Data mining, Data Warehouse.
5. In which areas of banking, the block chain technology can be used?
6. Who is Satoshi Nakamoto? Why he dislikes existing currencies?
7. What is the status of Crypto-currency in Bangladesh?
8. What is the present state of Crypto-currency in the world?
9. How Crypto-currency works? Narrate in details.
10. How many parties are involved in Crypto-currency?
11. What is the role of a miner in Crypto-currency production?
12. Who are the Crypto-currency end users?
13. What are the functions of an Online Wallet Providers?
14. What the Exchange Companies do?
15. What it is difficult to control Crypto-currency?
16. State the idea of introducing National Digital Currency? How it is different than Crypto-currency?
17. What is Artificial Intelligence? How Artificial Intelligence impact the banking?
18. What are the advantages of cloud banking? What are the challenges?
19. Describe current trend in banking in respect to technology use.

## References


1. Abul Kashem Md. Shirin and Nusrat Tamanna Prianka (2020): `Information Technology in Financial Services" 2nd Ed., The Institute of Bankers, Bangladesh (IBB)`.
2. Carol V. Brown, Daniel W DeHyes, Jeffrey Slater, Waingaert E. Martin: `Managing Information Technology`.
3. C.S. French, 1990: `Computer Studies, 3rd ed., Arnold Publishers, New Delhi, India`.
4. Graham Taylor, 2001: `GCSE Computer Studies, 4th ed., Macmillan Press Ltd., London`.
5. Grau, J. J. (ed.), 1992: `Criminal and Civil Investigation Handbook, 2nd ed., McGraw-Hill

   Inc., New York`.
6. Harry Bouwman, Bart Van den Hooff, Lidwein van de Wijngaert, Jan van Dijk: `Information and Communication Technology in Organizations`.
7. Indian Institute of Banking (IIB): `Electronic Banking and Information Technology`.
8. James A. O'Brien, 1999: `Management Information Systems, 4th ed., Tata McGraw-Hill Publishing Company Limited, New Delhi, India`.
9. Kenneth C. Laudon & Jane P. Laudon, 1999: `Management Information Systems – Organization and Technology, 4th ed., Prentice Hall of India, New Delhi – 110 001`.
10. Pete Loshin & Paul A. Murphy, 1999: Electronic Commerce, 2nd ed., Jaico Publishing House, Mumbai, India.
11. Wikipedia, 2010: `Wikipedia, the free encyclopedia on the internet on www.en.wikipedia.org/wiki/`.
12. Yekini Nureni: "Information Communication Technology (ICT)".