Digital Banking and Its Role in Preventing Cyber Fraud

Author: *SOUMADIP HALDER*
Date: *July 19th, 2025*

Table of Contents

1. Executive Summary

The rapid growth of digital banking has made banking easier and more accessible for both banks and customers. But at the same time, it has also created new ways for cyber-criminals to trick people and steal money. According to the report in 2024, bank around the worlds lost over **$28 billion** due to online fraud.

Key Highlights:

- Phishing attack increased by 85% and ATO cases rose by up to 60%.
- A four-layered security system is suggested which include smart login checks (MFA), behaviour tracking and monitoring tools and secure record-keeping using blockchain.
- Focus on catching fraud quickly, using strict security rules and teaching users about online fraud.
- Use of AI and machine learning is helping banks detect fraud patterns faster and reduce false alerts.
- Customer education and regular security training are becoming essential to reduce human error and social engineering risks.

2. Introduction

Digital banking is no longer just an option—it has become a vital part of how people manage their money. In recent years, digital banking services have changed with features like sending money through apps and applying for loans online. Using smartphones and the internet, people can now open accounts, pay bills, check balances, and invest—anytime from anywhere in the world. This has made banking easier especially after COVID-19 pandemic , when more people started using online services.

However, these changes also bring new risks. Cybercriminals are using smarter tricks to steal money and information. Some common threats include:

- **Phishing** (fake emails or texts asking for bank details)
- **Ransomware** (locking systems and asking for payment)
- **SIM swap fraud** (taking control of your mobile number)
- **Weak passwords or old systems**

Many older banking systems were not built for today's online attack. Also, as banks now connect with third-party apps through Open Banking, the risk of fraud grows if strong security is not in place.

In 2024, all the banks in world lost over **$28 billion** due to online fraud. That is why banks should not only make services easy to use, but also make them safe and keep customers protected. This report explains the growing online threats and suggests how banks can build stronger systems to protect customers and their data.

3. Background and Context

Evolution of Banking Channels

Era	Channel	Characteristics
Pre-2000s	Branch Banking	In-person visits, passbooks, manual entries
2000–2010	Internet Banking	Web-based portals, username-password access, early HTTPS adoption
2010–Present	Mobile Banking	App-first design, biometric login, API integrations, instant payments (like UPI, IMPS), cloud-based infrastructure

Key Points:

- According to report Between 2016 and 2024, India saw a 160 percent increase in mobile banking users due to smartphone adoption and affordable internet.
- As of 2023, over 80 percent of all banking transactions in India were done digitally (source: NPCI).
- QR code payments and UPI crossed 10 billion monthly transactions by late 2023, making India one of the largest digital payment markets globally.
- The shift from cash-based to digital-first banking has made speed and ease more important for banks.
- Banks are now investing more in API security and cloud infrastructure to handle increased digital traffic.

Banking Rules and Safety Guidelines

• RBI Digital Payment Security Framework (2025)

- Introduces strict rules for digital payment security, including customer authentication, fraud detection, and response timelines.
- Promotes the use of real-time monitoring, transaction risk scoring, and behavioral analysis.
- Encourages banks to adopt secure coding practices and regular cyber audits.

• Basel Committee Cyber Resilience Guidelines (2024)

- Suggests that banks use strong cybersecurity plans in their daily work.
- Advises banks to test their systems using fake attacks, check how well they can recover, and manage technology risks properly.
- Stresses the need for incident response plans and real-time threat sharing.

• EU General Data Protection Regulation (2018)

- Enforces customer consent for data collection and sharing.
- Requires reporting of data breaches within 72 hours.
- Non-compliance may result in fines up to 20 million euros or 4 percent of global turnover, whichever is higher.

4. Digital Banking Overview

Digital banking is the use of electronic platforms and devices to access and manage banking services. Over the last decade, it has become the primary way for people to interact with banks as smartphones, internet access, and user-friendly apps have made it easy.

Key Digital Services

• Online and mobile fund transfers through systems like IMPS, UPI, and NEFT have made real-time payments fast, easy, and available 24/7.

• Customers can apply for loans and complete credit checks entirely online, including paperless verification through e-KYC.

• Financial products like insurance, mutual funds, fixed deposits, and personal loans are now available through digital portals, removing the need to visit a physical branch.

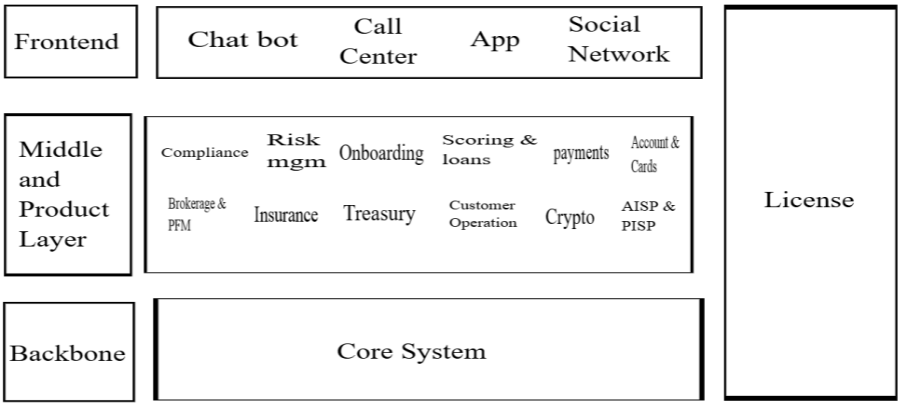
• Account statements, balance checks, and transaction alerts are available on-demand, often supported by AI-powered chatbots.

• Many banks also offer virtual debit cards, auto bill payments, and investment planning features through their digital apps.

Digital banking today covers almost every function that was once available only in person, and its use continues to grow rapidly across urban and rural areas alike.

Banking Tech Stack

Layer	Security practices
Frontend	Uses HTTPS, TLS 1.3 encryption for secure communication. Biometric authentication (like fingerprint or facial recognition) is used for app access.
Middleware	Responsible for connecting apps with databases and services. Uses protocols like OAuth 2.0 for secure access, along with tokenization and API rate limiting to prevent misuse.
Backend	Stores and processes sensitive data. Uses strong encryption methods such as AES-256 and separates data into secure zones to control access.
Operations	Relies on monitoring tools such as SIEM to detect threats. Includes storing logs, using real-time alerts, and gathering intelligence from external sources to prevent cyberattacks.



Simplified Overview of Banking tech stack

5. Cyber Fraud Landscape

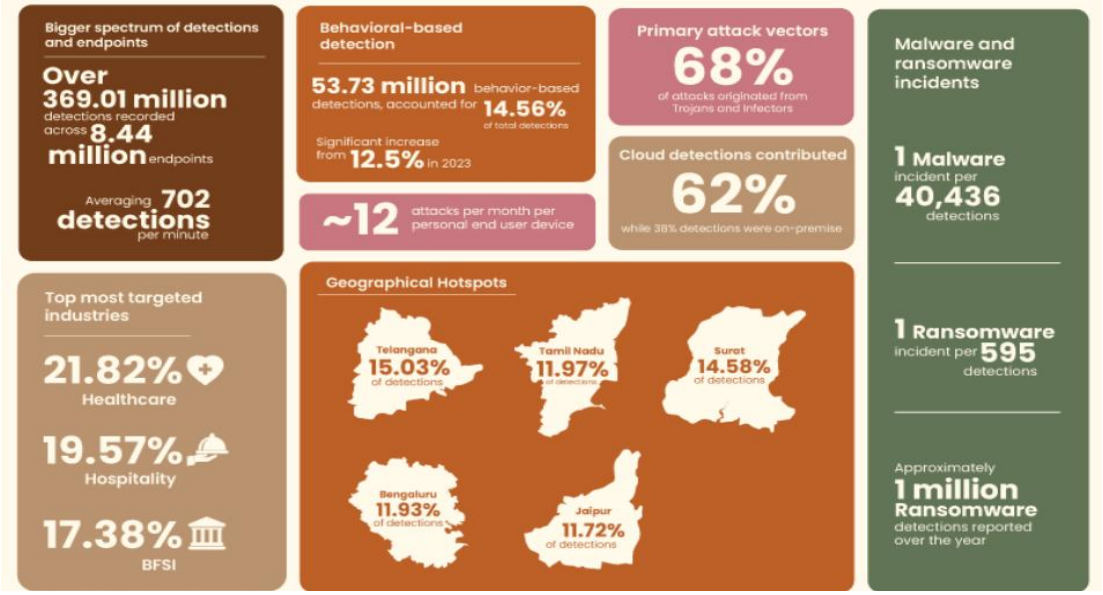
As more people use digital banking, the number of cyber fraud cases is also going up. Criminals use smart and tricky ways to steal money, personal information, or control of user accounts. Some of these attacks happen very quickly and are hard to notice until it's too late.

Fraud Type	Description
Phishing	Fake emails or messages trick users into clicking harmful links to steal their usernames, passwords, or OTPs.
ATO (Account Takeover)	Criminals gain access to a person's bank account by stealing login details or using SIM-swap tricks to get OTPs.
MITM (Man-in-the-Middle)	Hackers secretly listen to or change data between the user and bank while using public Wi-Fi or unsafe networks.
Ransomware	A virus that locks important files or systems and asks for money (ransom) to unlock them. This can stop banking services for hours or even days.

Trends (2024):

- Phishing cases went up by 85 percent as fake messages became harder to spot.
  (*Source: Keepnet Labs – Phishing Statistics 2024)*

- Account takeover fraud increased by 60 percent, often using leaked passwords or stolen SIMs.
- According to report The average money lost by a regular customer in a fraud was around 15,000 dollars.
- For banks and companies, a single attack caused losses of over 200,000 dollars.
- Ransomware attacks increased sharply, causing banks to shut down their systems for up to 2 days in some cases.



According to Report in India 17.38% Cyber Attack happen to BFSI

(Source :- https://www.dsci.in/resource/content/india-cyber-threat-report-2025)

6. Different Types of Cyberattacks :-

- **Phishing:**- A type of social engineering attack where attackers and fake emails, SMS pretending to be a trusted organization.
- **DDOS (Distibuted Denial-of-Service) :-** Attackers use multiple infected systems to flood a server or website with traffic, causing it to slow down or crash.
- **DOS (Deniel-of-Service**) :- A single attacker sends repeated requests to overload a system.
- **Malware (Malicious Software) :-** Malware is harmful software like viruses, spyware, and trojans that can break computers, steal information, or watch what users do.
- **Man-in-the-Middle :-** An attacker secretly intercepts and possibly alters communication between two parties**.**
- **SQL Injection:-** An attacker inserts harmful code into a form field (like login or search bars) to gain unauthorized access to the database.
- **Brute-Force-attack**:- The attacker uses software to try many combinations of usernames and passwords until they crack it.

7. Case Studies

PNB SWIFT Fraud – India (2018)

Overview:
At Punjab National Bank, some insiders used stolen login details to send fake Letters of Undertaking (LoUs) through the SWIFT system. They avoided the main banking software, which led to illegal money transfers of over $2 billion to other countries.

Root causes:
- SWIFT not connected to the Core Banking System (CBS)
- Lack of dual authorization for high-value messages
- Insider activity not monitored in real-time

Mitigation:
- RBI enforced mandatory SWIFT–CBS integration
- Introduced dual-control approval systems
- Improved internal access logs and audits

Reference:https://rbi.org.in/scripts/NotificationUser.aspx?Id=11243&Mode=0

Operation High Roller – Global (2012–2015)

Overview:
A worldwide malware attack took control of online banking sessions in over 60 banks by using fake screens and automatic programs.

Root causes:
- Sessions not validated properly
- No out-of-band (OOB) verification
- Static fraud detection systems failed to detect behavior anomalies

Mitigation:

- Behavioral profiling introduced
- Step-up authentication for risky actions
- Session tracking and browser fingerprinting implemented

Reference:https://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_41832.pdf

Lakshmi Bank Ransomware – (2022)

Overview:

A phishing email infected the bank's network, encrypting important data and stopping banking services for 48 hours.

Root causes:

- Unpatched systems left open to attack
- No internal segmentation to contain the malware
- Backups were online and also got encrypted

Mitigation:

- Regular patching and security updates applied
- EDR tools installed for early malware detection
- Backups moved offline and tested for recovery

Reference: https://csrc.nist.gov/publications/detail/sp/800-184/final

Zelle P2P Fraud – USA (2023–2024)

Overview:
Fraudsters posing as bank representatives convinced users to send money via Zelle, a popular P2P platform in the U.S., leading to major consumer losses.

Root causes:
- No fraud warning displayed before sending
- Social engineering tricks used to create urgency
- No way to reverse instant payments once approved

Mitigation:
- Banks added warning messages and confirmation steps
- Educated users about impersonation scams
- Delays added for new payees to allow fraud review

Reference: https://www.consumerfinance.gov/about-us/newsroom/cfpb-investigates-zelle-fraud-report-2024/

8. Analysis of Key Issues

A. Inadequate Authentication

- Static passwords and SMS-based OTPs are easy for attackers to compromise. For example, SIM swap fraud can intercept OTPs sent via SMS, giving attackers access to bank accounts
- Many systems do not include stronger protections like biometric checks or behavior-based login verification.

B. Alert Fatigue

- OC teams receive huge volumes of daily alerts. According to report it is around 4,484 per day. Around 67% of these alerts are ignored, mainly because they are false positives or low-priority.
- This constant flood of alerts means real threats can be missed, response times suffer, and staff experience high burnout.

C. Fragmented Monitoring

- Banks often have separate monitoring systems for mobile, web, and ATM platforms. This makes it difficult to detect fraud that moves across multiple channels.
- Because logs are scattered across different systems, it's hard to connect suspicious events in one channel with another. It slow down investigations and reducing visibility.

D. Insider Threats

- In general Privileged users such as administrators often have broad access, but their actions may not be tracked or monitored in real-time
- Without alerts for unusual admin behavior, internal misuse can go undetected for long periods. Studies show that many security problems are caused by people inside the company, and these are often missed because no one is watching closely.

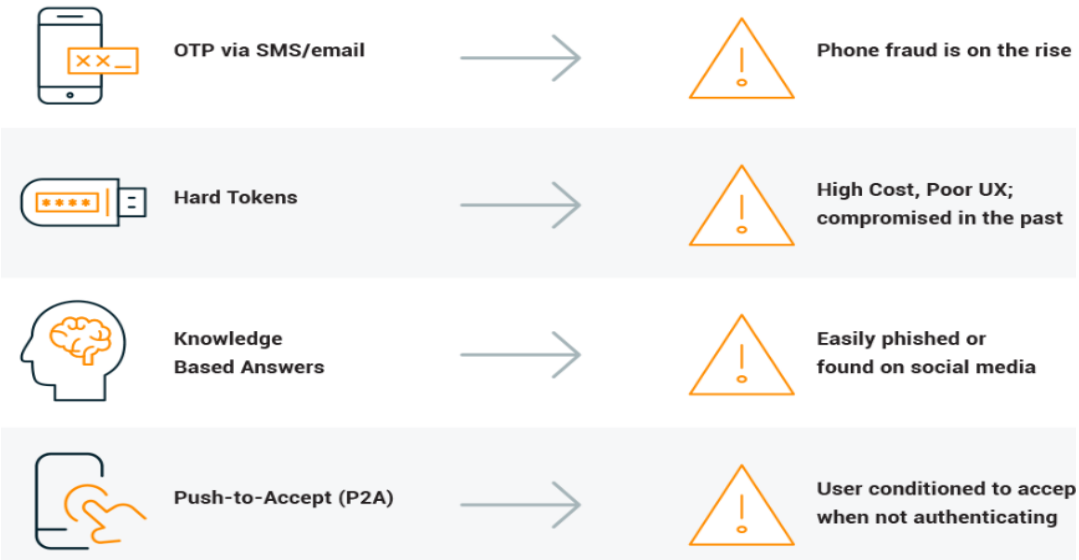
Why These Issues Matter

- Weak authentication makes it easy for attackers to bypass basic security.
- Alert fatigue disrupts threat detection and response—security teams are drowning in noise.
- Fragmented monitoring allows threats to move unnoticed across different banking channels.
- Insider threats remain invisible when system audits are delayed or inadequate.

9. Feasible Approaches

1. Adaptive Multi-Factor Authentication (AMFA)

- **How it works:** Evaluates risk based on factors like location, device, and IP, then decides whether to use password, OTP, biometrics, or step-up authentication.
- **Why it matters:** Offers strong protection while keeping the user experience smooth—extra checks only when needed. This reduces fraud without annoying customers (SecureAuth)
- **Benefits:** Balances security and convenience, helps banks comply with regulations, and limits fraud from remote logins.



2FA Method Can Bypass Easily and it is one of the possible Reason of Cyber Fraud in Bank. So, MFA can on strong possible Solution

2. Behavioral Biometrics

- **How it works:** Tracks the way users type, move their mouse, or swipe on mobile devices. These patterns help create a unique 'behavioral fingerprint' for continuous verification.
- **Why it matters:** Detects bots, fake sessions, and account takeover attempts as they happen. It runs silently in the background for better security without user interruption (Feedzai, LexisNexis).
- **Benefits:** Reduces false alarms, enhances fraud detection in real time, and helps identify money mule accounts and coerced transactions.

3. Unsupervised AI/ML

- **How it works:** Uses machine learning methods like Isolation Forests, One-Class SVM, clustering, or autoencoders to spot abnormal activity without needing labeled
- **Why it matters:** Detects new, unknown fraud patterns and adapts quickly. Banks don't need to predefine rules, and unusual transactions get flagged immediately (Medium, DataVisor).
- **Benefits:** Finds unusual transactions early—even ones never seen before—and helps cut losses while maintaining service speed.

4. Blockchain Audit Trails

- **How it works:** Stores transaction records in a tamper-proof blockchain, ensuring all changes are permanent, transparent, and resistant to alteration.
- **Why it matters:** Creates an immutable log for forensic audits and meets strict regulatory requirements. Helps track transaction history clearly and accurately.

(https://dev.to/kallileiser/unlocking-transparency-the-role-of-blockchain-audit-trails-in-modern-security-2mk8)

- **Benefits:** Prevents tampering, speeds up audit and compliance processes, and rebuilds trust through transparency.

These methods strengthen the four-layered defense model by improving authentication, monitoring behavior, detecting new types of fraud and ensure transparent record keeping.

10. Proposed Solution – Four-Layered Security Model

User Layer

- Adaptive MFA: Choose verification based on risk (e.g., use OTP only for high-risk actions).
- Continuous risk scoring: Systems assess each login and transaction, raising flags when risks increase (like unfamiliar location or device).
- Phishing awareness campaigns: Regular training and simulated phishing help users recognize and avoid scams.

Network Layer

- Enforce TLS 1.3 and HSTS: All data sent online is strongly protected, and websites are forced to use secure connections (HTTPS).
- Micro-segmentation: Network zones are limited and segmented to prevent lateral movement.
- IDS/IPS with anomaly detection: Monitor for unusual behavior and automatically block suspicious traffic.

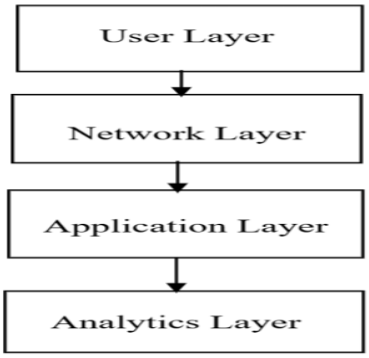
Application Layer

- Secure SDLC practices: Integrate static/dynamic code scanning and security tests within development cycles.
- Role-based access & privilege control: Define who can access what, enforcing least privilege and audit trails.

- API gateway with throttling & expiration: APIs are protected with rate limits, authentication, and token timing rules.

Analytics Layer

- Centralized SIEM ingestion (e.g. Splunk, ELK): Collect logs from all systems to identify events and trends.
- Real-time threat intelligence (e.g. Recorded Future): Update detection with the latest known TTPs and indicators of compromise.
- SOAR for response automation: Automate common responses like blocking IPs, isolating devices, or notifying admins.

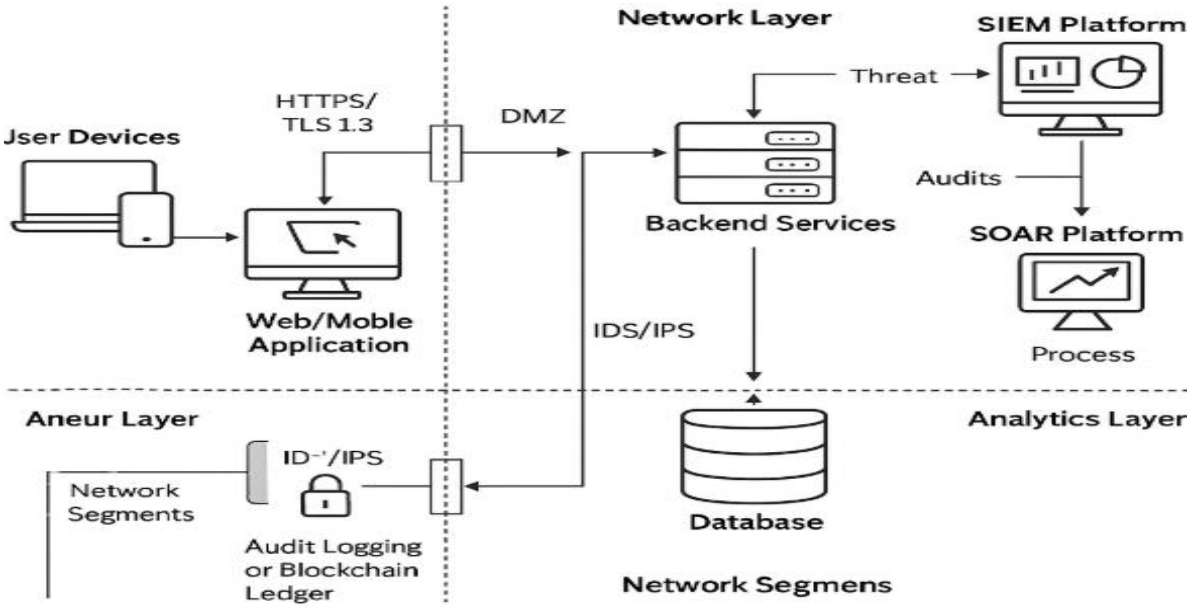


Four Layered Model

Architecture Overview

1. **User devices** connect securely via HTTPS over TLS 1.3 to the **web/mobile application**.
2. **API Gateway** processes requests with authentication, rate limits, and forwards to backend services.
3. **Backend Services** run within the App zone with defined access to encrypted databases.

4. **Network Segments**: Core, DMZ, and App zones communicate via strict firewalls.
5. **IDS/IPS systems** monitor and enforce network security.
6. **SIEM Platform** receives logs from all components, enriching them with threat feeds and applying correlation rules.
7. **SOAR Platform** responds automatically to rules violations or anomalies using pre-configured playbooks.
8. **Audit logging or blockchain ledger** captures immutable records of all transactions and sensitive operations for forensics and compliance.



Architecture of the Four-Layered Security Model

11. Implementation Plan

Phase	Duration	Milestone	Details
1	Months 1–2	Vendor evaluation	• Evaluate SIEM, SOAR, and MFA solutions. • Define security policies based on RBI/GDPR. • Assign internal teams and design architecture.
2	Months 3–5	Pilot testing	• Test tools in a controlled environment. • Simulate phishing and ATO attacks. • Collect team feedback for adjustments.
3	Months 6–10	Full rollout, team training	• Deploy solution across all platforms. • Train SOC, fraud teams, and IT staff. • Integrate with apps, APIs, and backend systems.
4	Months 11–12	Performance audit, ML tuning	• Conduct fraud detection and alert accuracy review. • Tune ML models using real incident data. • Finalize executive reports and compliance checks.

12. Risk Assessment

Risk Type	Likelihood	Impact	Mitigation Strategy
Model Drift	Medium	High	Machine learning models may become outdated because fraud patterns change day by day. Retrain models using recent fraud data to maintain detection accuracy.
Integration Delay	High	Medium	Delays may occur while connecting new tools to legacy systems. Use an agile rollout approach with fallback support to avoid full system disruption.
GDPR Violation	Low	High	Mishandling of user data may lead to legal fines and reputation loss. Conduct regular audits and enforce data handling policies to ensure compliance.

13. Monitoring and Evaluation

A strong fraud prevention system is only effective if it is continuously monitored and evaluated. This ensures that any weaknesses are quickly identified and improvements are made over time. Monitoring helps detect issues early, while evaluation measures how well the system is performing.

Metrics

- **Fraud loss reduction :-**
  This measures the percentage decrease in the total financial loss due to fraud after implementing the new security measures. A consistent decline indicates that the system is effectively blocking fraud attempts.
- **Mean Time to Detect (MTTD):**
  This is the average time taken from the start of a fraud incident until it is detected. A shorter MTTD means faster awareness and quicker action, which reduces potential damage.
- **False-positive ratio:**
  This tracks the number of times the system flags a legitimate transaction or user as fraudulent. Reducing false positives is important because too many of them can overwhelm the fraud team and reduce customer satisfaction.

Tools

- **SIEM dashboards (e.g. :- Splunk, ELK):**
  Security Information and Event Management (SIEM) systems collect logs and security data from across the network. Dashboards help security teams visualize threats and investigate incidents in real-time.

- **SOAR orchestration tools (e.g. :- IBM QRadar SOAR, Palo Alto XSOAR):**
  These tools help automate the response to incidents. For example, if a login attempt looks suspicious, the SOAR platform can automatically disable the account, send alerts, and begin an investigation without waiting for manual action.
- **Audit trail and anomaly correlation engines:**
  These systems record every major action taken across user accounts, applications, and networks. They link related activities to spot patterns of fraud and help during forensic analysis or compliance reviews.

Cadence

- **Daily:** SOC monitoring
  The Security Operations Center (SOC) continuously monitors for alerts, unusual logins, failed transactions, or other suspicious activity. Daily monitoring ensures real-time threat detection**.**
- **Weekly:** Risk review reports
  A detailed report is prepared and reviewed by the risk and compliance team every week. It includes summaries of incidents, response actions, system performance, and any changes in fraud trends.
- **Quarterly:** Strategic security audits
  Every three months, a comprehensive audit is conducted to evaluate the effectiveness of the overall security strategy. This includes reviewing tool performance, updating threat detection rules, and aligning processes with new regulatory requirements.

14. Conclusion

Digital banking is growing rapidly, but it can only succeed if customers trust that their money and personal information are safe. Today, cyber fraud is becoming more advanced, and banks need to be smarter in how they protect users and systems.

The four-layered security model—made up of the **user layer**, **network layer**, **application layer**, and **analytics layer**—gives full protection from different kinds of threats. Each layer adds an extra shield so that if one fails, others still protect the system.

Key Points:

- Modern threats need smart and ongoing monitoring
  Fraud can happen in new ways every day. Banks need systems that learn user behavior and quickly find anything unusual.

- Teaching users and staff is very important
  Training people to spot fake emails or messages helps reduce mistakes and prevents fraud before it starts.

- Using AI tools helps detect fraud faster These tools cut down the time needed to respond and help teams focus on real problems.

- Regular checks keep the system strong By reviewing how well security tools are working, banks can improve over time and stay ahead of threats.

- Following rules and laws protects both banks and customers Staying in line with RBI, GDPR, and other guidelines keeps the bank legally safe and builds trust with users.

Using this approach, banks can stop fraud before it happens, keep users safe, and grow their digital services with confidence. Good cybersecurity is not just a choice—it is the base for a safe and successful future in digital banking.

A strong, multi-layered security system helps banks stay prepared for both known and new types of attacks. It builds trust with customers, reduces financial losses, and ensures smooth day-to-day operations. As more people depend on digital platforms for payments, loans, and investments, the need for reliable protection becomes even more important.

In the future, banks that use smarter security, check systems regularly, and teach users how to stay safe will grow faster. These banks will lead in digital change. Cybersecurity is not just a tech job now. It helps build trust, protect people, and create a strong and safe brand.

15. References

1. Basel Committee – Cyber Resilience Guidelines (2024)(https://www.bis.org/bcbs/events/icbs24/icbs24_workshop3.pdf)

2. NIST SP 800-184 – Guide for Cybersecurity Event Recovery (2022) (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf)

3. GDPR Portal (2018) (https://gdpr.eu)

4. SecureAuth – *Importance of Adaptive Authentication in Financial Services* (Aug 15, 2024)(https://www.secureauth.com/resources/importance-of-adaptive-authentication-in-financial-services)

5. SOFTwarfare – *Securing the Future of Banking Through Adaptive Authentication* (Mar 2025)(https://blog.softwarfare.com/securing-banking-with-adaptive-authentication)

6. Medium – *Risk-Based Authentication (RBA): Enhancing Security with Adaptive Identity Verification* (Feb 22, 2025) (https://medium.com/o-m-n-i-navigating-the-new-cyber-era/risk-based-authentication-rba-enhancing-security-with-adaptive-identity-verification-80d0e83f875b)

16. Abbreviations

Acronym	Full Form
AI	Artificial Intelligence
ATO	Account Takeover
KYC	Know Your Customer
MFA	Multi-Factor Authentication
OTP	One-Time Password
SIEM	Security Information and Event Management
SOAR	Security Orchestration and Automated Response
GDPR	General Data Protection Regulation
RBI	Reserve Bank of India
AMFA	Adaptive Multi-Factor Authentication
MITM	Man-in-the-Middle
CBS	Core Banking System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SDLC	Software Development Life Cycle

Acronym	Full Form
API	Application Programming Interface
ELK	Elasticsearch, Logstash, and Kibana
MTTD	Mean Time to Detect
DMZ	Demilitarized Zone (Network)
OOB	Out-of-Band (Authentication)
EDR	Endpoint Detection and Response
URL	Uniform Resource Locator

17. Acknowledgements

I would like to sincerely thank **the Reserve Bank of India (RBI)**, **CERT**-In, the **Basel Committee**, **SEI CERT**, and **NIST** for sharing useful reports, research papers, and public resources. Their information helped me a lot in making this report.

Their data, case studies, and technical guidelines helped me understand the real-world impact of cyber fraud and the importance of strong digital banking security.

I am also very thankful to my mentor Chief Manager **shri Rupal Kumar**, whose initial guidance, feedback, and encouragement were extremely helpful throughout this project. Their suggestions helped me stay focused and improve the quality of my research.

Lastly, I would like to thank all the cybersecurity experts, financial analysts, and institutions whose articles, tools, and frameworks helped shape this comprehensive study.

18. Appendices

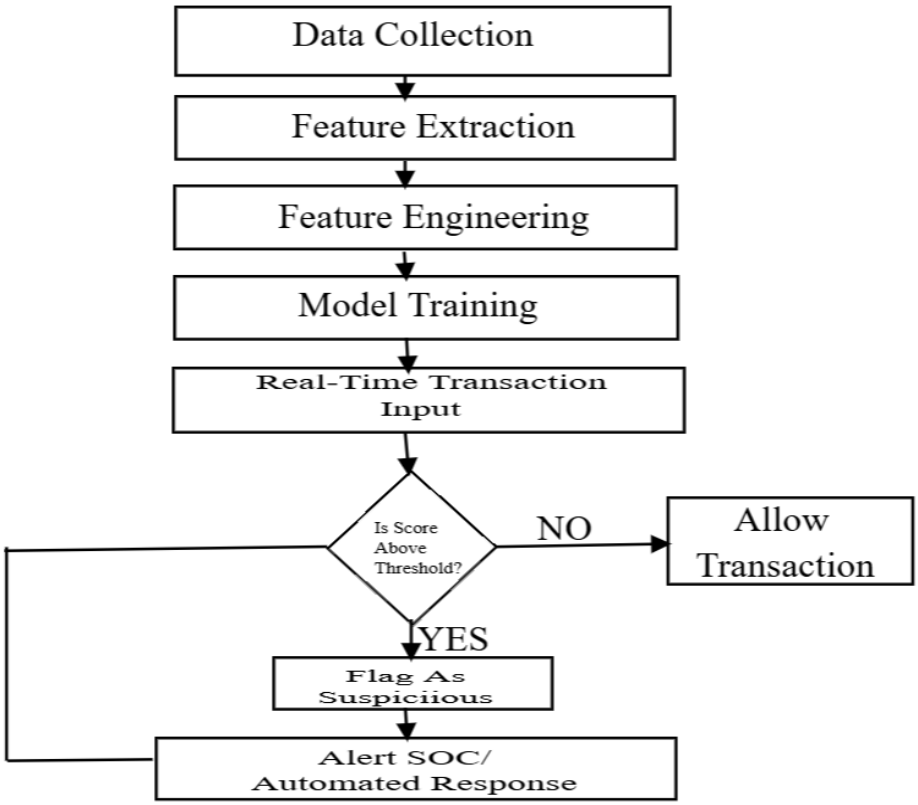
Appendix A: Glossary of Cybersecurity Terms

This section includes definitions of key terms used in the report to help readers understand basic cybersecurity concepts.

- **Phishing:** A type of cyberattack where fake emails or messages are sent to trick users into giving away sensitive information like passwords or banking details.
- **Sandboxing:** A security method that runs suspicious programs in an isolated environment to see if they are harmful without affecting the actual system.
- **Tokenization:** The process of replacing sensitive data (like card numbers) with random tokens, making it unreadable to attackers.
- **TLS (Transport Layer Security):** A protocol used to secure data sent over the internet, such as between a banking app and the server.
- **Malware:** Malicious software designed to damage, steal, or disrupt computer systems (e.g., ransomware, spyware, viruses).
- **Segmentation:** Dividing a network into smaller parts to limit the spread of threats and control access.

Appendix B: ML Fraud Detection Flowchart

Steps from data collection → feature extraction → anomaly scoring → response trigger.



Appendix C: Phishing Simulation Template

This appendix provides an example of a fake email that can be used to test employee awareness and conduct training.

Subject: Important: Urgent Update Required for Your Bank Account
From: security-notice@bankalerts.com

Dear Customer,

We have detected unusual activity on your account. To ensure uninterrupted access, please confirm your identity by clicking the secure link below:

Verify Now

Failure to act within 24 hours will result in temporary suspension of your services.

Thank you,
Cybersecurity Team
Your Bank Ltd.

Red Flags to Train Users To Spot:

- Generic greeting (“Dear Customer”).
- Sense of urgency (“24 hours”).
- Suspicious link (hover to reveal mismatched URL)
- Grammatical issues or typos.