CYBER SECURITY IN FINANCE

- Kunal Singh[1] & Rushali Pandey[2]

INTRODUCTION

The rapid digitalization of the banking industry has entirely reshaped the landscape of banking, payment systems, and financial transactions and made them more convenient, efficient, and user-friendly. But this digitalization has also brought harsh cybersecurity issues, as banks are being targeted as prime targets by cybercriminals. Cybersecurity has become a big issue for banks, fintech operators, regulatory bodies, and customers, as there is a steady pace of evolution in the sophistication and frequency of cyber threats. The increased reliance on online banking, mobile payment systems, cryptocurrency transactions, and cloud-based financial services has led to a massive surge in cyberattacks to steal sensitive customer data, interfere with banking activities, and manipulate financial systems.

In India, the financial sector has witnessed exponential growth in digital adoption, driven by programs such as Digital India and Aadhaar-based financial inclusion that facilitate rapid digital penetration. Technologies such as the Unified Payments Interface (UPI), mobile banking, and fintech solutions have made financial services more accessible; however, they have also increased the risk of cyberattacks. High-profile cyberattacks, such as the Cosmos Bank cyber heist and the Aadhaar data breach, have identified weaknesses in India's financial ecosystem, highlighting the urgent need for end-to-end cybersecurity solutions. Consequently, the Reserve Bank of India (RBI) and other regulatory bodies have enforced strict cybersecurity regulations, forcing banks to enhance their security frameworks through real-time monitoring, risk assessment, and incident response plans. Nevertheless, financial institutions are still susceptible to repeated attacks such as phishing, ransomware attacks, identity theft, and ATM skimming despite such regulatory policies. Cyber attackers use advanced methods, such as AI-powered cyberattacks, deepfake scams, and supply chain attacks, to breach financial systems. Additionally, the emergence of new threats in the form of quantum computing poses potential threats to current encryption methods, for which financial institutions need to deploy cutting-edge security measures. Today, AI-powered fraud detection systems, blockchain-protected

[1] Kunal Singh, 1st Year Law Student, National Forensic Sciences University, Gandhinagar.
[2] Rushali Pandey, 1st Year Law Student, D.Y. Patil College of Law, Mumbai.

transaction methods, and quantum-resistant cryptographic methods are increasingly deployed into financial security systems to combat such new threats.

This essay discusses the key aspects of cybersecurity in the banking industry, such as cyber threats, empirical case studies, security best practices, regulatory directives, and future-proof cybersecurity solutions. The focus is to offer a comprehensive insight into how banking institutions can overcome cyber threats and offer a safe and robust digital banking environment in India and internationally. As cyberattacks evolve and become more widespread, financial institutions must stay ahead of upcoming threats by taking proactive defence mechanisms and continuous updates in security controls.

CYBER SECURITY

Cybersecurity refers to the practice of protecting digital systems, networks, and financial data from unauthorized access, cyberattacks, and breaches. In the financial sector, cybersecurity is particularly crucial as banking institutions manage vast amounts of sensitive personal and financial information. Cybersecurity measures include encryption, network security protocols, secure authentication methods, compliance with legal frameworks, and using artificial intelligence for fraud detection. Banks, fintech firms, insurance companies, and stock exchanges all rely on cybersecurity to protect customer transactions, maintain trust, and ensure the financial system's stability. The increasing digitization of financial services has led to the proliferation of cyber threats, making it imperative for financial institutions to strengthen their security infrastructure and implement best practices to mitigate risks.

TYPES OF ATTACKS

Anti-Fraud Bypass: The increasing volume of online transactions has led to cybercriminals abusing hacked biometric information, such as fingerprints and facial recognition, to circumvent security controls. This functionality enables them to impersonate legitimate users and execute unauthorized transactions. Financial institutions must strengthen authentication processes and continually update fraud detection systems in response to these changing threats.

ATM Malware: Malware is used by cybercriminals to take control of ATMs and enable unauthorized cash withdrawals. Black box devices, software vulnerabilities, and card

skimming are used to conduct such attacks. Software updates, encryption, and real-time monitoring are required to prevent fraud.

Phishing: Phishing attacks deceive users into revealing sensitive information through spurious emails, websites, or phone calls. Attackers gain access to victims' accounts once victims unknowingly provide login information. Suspecting links, authenticating source communications, and enabling two-factor authentication would avert threats.

Account-Based Frauds: Hackers obtain unauthorized access to bank accounts using weak passwords, credential stuffing, or SIM swapping. Once they have entered, they conduct fraudulent transactions or steal customer data. Strong passwords, multi-factor authentication, and regular account checking avoid such breaches.

Identity Theft: Cybercrooks use the obtained personal details to create fraudulent accounts, secure loans, or pretend to be victims of money fraud. Regularly checking financial statements and avoiding excessive online posting of sensitive information can reduce the threat of identity theft.

Employee Threats: Dissatisfied staff with access to confidential information may leak the information, corrupt systems, or engage in fraud. Businesses must impose stern access controls, surveil internal operations, and ensure cybersecurity knowledge to avert insider threats.

Ransomware: Hackers encrypt financial information and ask for ransom for its release, attacking institutions with legacy security systems. These attacks are a disruption and lead to financial loss. Frequent data backups, robust cybersecurity infrastructure, and employee sensitization can reduce the risk of ransomware attacks.

SIGNIFICANT SECURITY BREACHES IN FINANCIAL INSTITUTIONS

The Bangladesh Bank Heist (2016): Hackers exploited vulnerabilities in the SWIFT financial messaging system to steal $81 million from Bangladesh Bank's account at the Federal Reserve Bank of New York. The attack involved sending fraudulent SWIFT messages to transfer funds to accounts in other countries. This breach highlighted the need for stronger authentication and monitoring mechanisms in financial messaging systems

UIDAI: One of the most significant data breaches in the world was reported in 2018 when the Aadhar card details of 1.1 billion citizens were leaked in India. The Unique Identification

Authority of India (UIDAI) officially announced its data breach through notification and mentioned the hacking of over 210 websites by the Government of India. Hackers stole details like PAN, Aadhar number, IFSC codes of bank accounts linked with Aadhar, and other citizens' private data. It was also observed that anonymous sellers were selling Aadhar information over WhatsApp for Rs. 500. Even worse, one could print out fake Aadhar cards for only Rs. 300.

Canara Bank ATM: In 2018, hackers targeted Canara Bank ATM servers. They stole the ATM details of over 300 users and siphoned over Rs. 20 lakhs from several accounts. They stole Rs. 20 Lakh using skimming devices on ATMs. This way, banks should enhance their ATMs' security features to avoid such incidents in future.

Cosmos Bank, Pune: In 2018, Pune-based Cosmos Bank suffered an attack where attackers hacked into the ATM server of the bank, stole all the card details, drained off Rs. 94.42 crores and withdrew the amount quickly from 28 countries. Hence, authorized people must strengthen their security systems.

JP Morgan Chase Breach (2014): Cybercriminals gained access to the personal information of 83 million customers by exploiting a vulnerability on JP Morgan Chase's website. The breach involved compromising user accounts and accessing sensitive data, including email addresses and account numbers. The incident highlighted the need for robust web application security and effective response mechanisms.

BEST PRACTICES FOR SECURING FINANCIAL SYSTEMS

Encryption And Secure Communication Protocols: Encryption protects financial transactions by ensuring data confidentiality and integrity during transmission. Advanced Encryption Standards (AES) and Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols are the most used encryption techniques. AES, a symmetric key encryption algorithm, provides strong security for encrypting financial information. On the other hand, SSL/TLS protocols provide encrypted communication channels between clients and servers to ensure secure data transmission. Such encryption technologies keep data safe and block unauthorized access while safeguarding confidential financial data. For example, online banking sites employ SSL/TLS encryption to secure data communicated between a client's browser and the bank's server to prevent interception or tampering.

Multi-Factor Authentication (MFA): MFA enhances security by requiring users to provide multiple verification forms. Typically, MFA includes something the user knows (password), something they have (security token or smartphone app), and something they are (biometric verification). MFA significantly reduces the risk of unauthorized access by adding additional layers of security.

Biometric Authentication: Biometric technologies, such as fingerprint scanning, facial recognition, and iris scanning, offer advanced security by verifying unique physical characteristics. Biometric authentication is becoming increasingly popular in financial services due to its convenience and high security. For example, fingerprint authentication is commonly used in mobile banking apps to provide secure access to financial accounts.

Intrusion Detection and Prevention Systems: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are critical components in the security of financial systems, as they track network activity and block cyber threats. IDS detects and notifies administrators of suspicious activity, while IPS actively blocks malicious traffic before causing harm. These systems employ various detection methods, including signature-based detection, which identifies known attack signatures; anomaly detection, which identifies abnormal behaviour; and heuristic analysis, which analyses activity to detect new or emerging threats. Effective deployment of IDS and IPS facilitates real-time threat detection and response, improving overall cybersecurity.

Blockchain Technology and Its Impact on Financial Security: Transactions without the need for intermediaries. This can reduce transaction costs and increase the efficiency of financial operations. Additionally, blockchain's transparent ledger allows for real-time tracking of transactions and auditing, making it easier to detect and address fraudulent activities. Several financial institutions have begun exploring blockchain technology to enhance security measures. For instance, Ripple's blockchain-based payment system offers faster and more secure international money transfers by providing a transparent and immutable record of transactions. Similarly, JPMorgan Chase has developed its blockchain platform, Quorum, to facilitate safe and efficient financial transactions.

EMERGING TECHNOLOGIES FOR SECURING FINANCIAL SYSTEMS

Blockchain Technology: Blockchain technology offers a decentralized and immutable ledger for recording transactions, which enhances security and transparency in financial operations. By distributing its data across a network of computers, blockchain makes it extremely difficult

for hackers to compromise the integrity of the economic data. The technology's inherent characteristics, such as immutability and transparency, ensure that it cannot be altered once a transaction is recorded, fostering trust among participants. Blockchain finds application in various aspects of finance, including cryptocurrencies like Bitcoin, which introduced a new paradigm for digital currencies; smart contracts that automatically execute agreements without intermediaries; and secure data sharing, which allows for the confidential and tamper-proof exchange of information. Despite its potential, blockchain's adoption faces scalability issues, energy consumption concerns, regulatory uncertainties, and the challenge of integrating with existing financial systems. These factors need to be addressed to leverage blockchain in financial services fully.

Artificial Intelligence and Machine Learning: AI and ML are revolutionizing cybersecurity in financial institutions by enabling advanced detection and response mechanisms. AI and ML are used for fraud detection by analysing transaction patterns to identify anomalies that indicate fraudulent activity. They also support anomaly detection beyond transactions, such as user behaviour or network traffic, and contribute to threat intelligence by predicting and identifying emerging cyber threats. AI-driven security solutions offer the benefit of speed and efficiency, allowing financial institutions to identify and respond to threats faster than humanly possible. However, these technologies also come with risks. One is the potential for false positives that can disrupt legitimate transactions, a model bias that may result from training data and the susceptibility to adversarial attacks designed to deceive AI systems.

Quantum-Safe Cryptography: The advent of quantum computing poses a significant threat to traditional cryptographic algorithms, necessitating the development of quantum-safe cryptography. Quantum computers, with their ability to solve complex mathematical problems much faster than classical computers, could eventually break many cryptographic algorithms currently used to secure financial data, rendering traditional encryption methods obsolete. To counteract this potential threat, a growing focus is on developing quantum-resistant cryptographic algorithms to secure sensitive financial information against future quantum attacks. This includes research into post-quantum cryptography, which aims to create encryption methods that quantum computers cannot easily break. Various international organizations and research bodies are actively working on developing standards for quantum-

safe cryptography. These efforts ensure a smooth transition to quantum-resistant cryptographic practices, safeguarding financial transactions and data against future quantum threats.

NIST Cybersecurity Framework: Among the recommended best practices for enhancing cybersecurity in the financial industry is the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This world-renowned framework offers a systematic method of managing cybersecurity risk using five core functions: Identify, Protect, Detect, Respond, and Recover. This model can be applied by financial institutions to determine their security stance, apply safeguarding measures, identify cyber threats in real time, and set effective incident response policies. By adhering to NIST guidelines, banks and fintech companies can become more resilient against cyber threats, achieve better regulatory compliance, and reduce financial losses from cyber-attacks.

CONCLUSION

Cybersecurity is at the forefront of safeguarding financial transactions and maintaining confidentiality, integrity, and availability of financial information. With financial institutions still evolving and embracing digital banking, the demand for dynamic and robust cybersecurity arrangements grows more vital. No technology or framework can offer total protection against cyber threats; institutions need to adopt a multi-layered system, constantly enhancing security arrangements to fight evolving threats.

As a developing nation, India is going great guns in computerizing its banking industry, enabling customers to make transactions anytime, anywhere through mobile phones, laptops, or cards. While convenience is improved with this computerization, it also brings with it new vulnerabilities. Banks must assure customers that their money and personal information are safe by adopting strong security features, undertaking frequent security checks, and ensuring adherence to cybersecurity guidelines. Before introducing new financial technologies, banks must extensively test security measures to avoid cyber-attacks and data breaches.

However, cybersecurity protection is not only in the hands of financial institutions. Consumers themselves have a part to play in ensuring cyber cleanliness. It becomes essential for customers to keep their devices malware-free, install virus-guard software, refrain from downloading applications from unknown sources, and be extremely careful about avoiding phishing. In case

of an unauthorized transaction, it should immediately be reported to the concerned finance authorities to preclude any further damage.

As cyber threats constantly change, financial institutions must be alert and proactive, continually evolving to keep up with technological developments and new risks. Future studies must address the gaps in cybersecurity frameworks and investigate new solutions to secure financial transactions. While an entirely foolproof cybersecurity plan might not be possible, the interplay between robust institutional controls and public awareness can help stem risks and create a more secure financial system. By creating a cybersecurity sensitivity and resilience culture, financial institutions and clients can collaborate to construct a safe and reliable digital banking space.