Cyber Security in Banking Security System

Aradhya. S.R.
Vishwa Chethana Degree college, Anekal, Karnataka.

***Abstract*—Automated Teller Machines (ATMs), electronic payment systems, mobile banking, and online banking all contributed to the banking industry's quick digital transition. While these technologies enhance exposure to cyber dangers such phishing assaults, malware, ransomware, data breaches, identity theft, and financial fraud, they also improve efficiency and customer convenience. As a result, cybersecurity has emerged as a crucial prerequisite for safeguarding financial transactions, consumer data, and banking infrastructure. Firewalls, intrusion detection and prevention systems (IDS/IPS), encryption, multifactor authentication, Security Information and Event Management (SIEM), and network security monitoring are just a few of the cybersecurity techniques used by banking security systems. Together, these technologies guard against illegal access, identify harmful activity, and guarantee the availability, confidentiality, and integrity of banking services. By providing real- time fraud detection, customer authentication, anomaly detection, behavioral analysis, and predictive threat intelligence, recent developments in artificial intelligence (AI) and machine learning (ML) have greatly boosted banking cybersecurity. Large amounts of transaction and network data may be analyzed by AIdriven systems, which can also spot suspicious patterns and react swiftly to new risks. AI and ML are used in ATM security to identify anomalous transaction behavior, malware attacks, unauthorized access, and card skimming. This paper explores the role of cutting-edge technology in protecting digital financial services and emphasizes the significance of cybersecurity in contemporary banking systems. Banks can increase threat detection, improve incident response, lower fraud risks, and offer clients safe and dependable services by combining traditional security controls with AI-powered solutions. Maintaining consumer confidence, adhering to regulations, and the general viability of the banking industry all depend on effective cybersecurity procedures.**

I. INTRODUCTION

Offering financial services. A like deposits, loans, cash transfers, internet banking, mobile banking, and ATM transactions, the banking sector is one of the most significant in the world economy. Banks now rely more and more on computerized systems and network infrastructures due to the quick development of digital technologies and internet-based financial services. Digital transformation has boosted client convenience, accessibility, and efficiency, but it has also raised the possibility of security breaches and cyberattacks. In the banking industry, cybersecurity refers to the set of technology, rules, processes, and practices used to guard against financial fraud, cyberattacks, and illegal access to banking systems, networks, apps, and consumer data. Because banks hold sensitive client data, financial records, and valuable digital assets, they are appealing targets for cybercriminals. Phishing attacks, malware, ransomware, identity theft, data breaches, Distributed Denial-of-Service (DDoS) assaults, insider threats, and ATM-related fraud are among the many cyberthreats that banks must deal with. Banks use a variety of security measures, such as firewalls, encryption, intrusion detection and prevention systems (IDS/IPS), Security Information and Event Management (SIEM), multifactor authentication (MFA), network monitoring, and access control techniques, to solve these issues. These security precautions aid in guaranteeing the availability, confidentiality, and integrity of banking data and services. Machine learning (ML) and artificial intelligence (AI) have become potent tools for improving banking cybersecurity in recent years. Real-time fraud detection, behavioral analysis, customer identification, anomaly detection, and predictive threat intelligence are all made possible by these technologies. AI-driven systems can analyze enormous volumes of data, spot suspicious activity, and react fast to possible attacks, all of which improve banking organizations' overall security posture.

II. OBJECTIVES OF THE STUDY

1. To analyse different types of cyber threats and attacks affecting banking security systems.

2. To examine the existing cyber security measures adopted by banks to protect customer data and financial transactions.
3. To study the role of technologies such as encryption, firewalls, multi-factor authentication, and intrusion detection systems in banking security.

III. RESEARCH METHODOLOGY

This study's methodology, which is based on a qualitative and descriptive research approach, focuses on examining the body of knowledge regarding cyber security in the banking industry. To describe contemporary cyberthreats and security measures without changing any variables, a descriptive study design is employed. The study makes use of secondary data gathered from online academic databases, research papers, journals, and reports. It also entails analyzing cybersecurity techniques like blockchain, multi-factor authentication, firewalls, IDS, encryption, and AI-based fraud detection while recognizing their drawbacks including dependence on secondary data and quickly evolving cyberthreats.

IV. REVIEW OF LITERATURE

The fast expansion of digital banking services including internet banking, mobile banking, and online payment systems has made cyber security in the banking industry a crucial field of study. Financial institutions are more susceptible to ransomware, phishing, malware assaults, identity theft, and illegal access as a result of their growing reliance on digital platforms. Numerous scholars have examined these issues and suggested ways to improve banking security systems. Phishing and malware attacks continue to be the most popular ways for cybercriminals to take advantage of banking systems, according to a comprehensive assessment on cybersecurity threats in digital banking. According to the report, authentication systems are a major security risk since hackers frequently use harmful software and phony websites to target client credentials (SSRN, 2025). This highlights the necessity of user awareness campaigns and more robust multi-factor authentication in financial operations. Another study that was published in Expert Systems with Applications (Elsevier) evaluates several protection strategies employed in FinTech contexts and classifies numerous cyberthreats that impact financial systems. According to the study, banking systems are vulnerable to both internal (such as staff carelessness or insider assaults) and external (such as hackers, malware, and phishing) risks. To lower risks, it recommends using real-time monitoring tools and intrusion detection systems based on artificial intelligence. The significance of encryption technology and secure communication protocols is further highlighted by research on protecting financial transactions in banking systems. It clarifies that safeguarding data during online transactions is crucial to avoiding hackers' interception and manipulation. In order to increase transaction security, the study also covers identity verification methods such token-based authentication and biometrics. Furthermore, research on the effects of cybercrime in the banking industry reveals that cyberattacks harm a company's reputation and consumer trust in addition to causing financial losses. Regulatory fines and a decline in consumer trust are common outcomes for banks that encounter repeated cyber breaches. This emphasizes how crucial it is to keep robust cybersecurity policies in order to guarantee confidence in digital banking systems. According to research on mobile banking security and privacy, poor application architecture and lax authentication procedures make mobile applications especially vulnerable. The report suggests using secure coding techniques, biometric authentication, and frequent vulnerability checks to increase application security. Blockchain technology and artificial intelligence are being used more frequently in financial systems, according to recent developments in cybersecurity research. Blockchain offers decentralized and impenetrable transaction records, while AI is utilized for automated threat response, anomaly identification, and fraud detection. The resistance of banking security systems to contemporary cyberthreats is greatly increased by these technologies. Overall, research indicates that although financial systems have implemented a number of security measures, cyber dangers are ever evolving. Therefore, in order to guarantee secure banking operations, there is a constant need for more sophisticated technology, robust authentication mechanisms, and raised customer awareness.

V. COMMON CYBER THREATS IN BANKING

5.1. Phishing Attacks

Fraudulent websites, emails, or communications intended to obtain user credentials.

5.2. Attacks by Trojans
A Banker Trojan appears to be reliable software until it is installed on a computer. Nevertheless, it is a malicious computer program designed to gain access to personal information handled or stored by online banking systems. A backdoor in this type of computer program allows external access to a computer.

5.3. Spoofing
By copying the item, it is similar to hacking.

5.4. Ransomware and malware malicious malware that can lock systems until a ransom is paid or steal data.

5.5. Data breaches include unauthorized access to private financial and customer data.

5.6. Attacks using Distributed Denial of Service (DDoS) Overloading financial servers to the point where services are unavailable.

5.7. Insider Dangers Workers or contractors who inadvertently or purposely jeopardize security.

5.8. Fraud involving ATMs and credit cards Methods like unapproved transactions and card skimming.

VI. SECURITY MEASURES USED BY BANKS TO PROTECT FROM THE CYBER THREATS

6.1 Multi-Factor Authentication (MFA): A cybersecurity technique known as multi-factor authentication (MFA) requires users to supply two or more verification factors in order to get access to an account, system, or application. It provides more security than a password alone.

Common MFA Methods

MFA Method	Example
SMS Code	OTP sent to phone or Email
Authenticator App	Google Authenticator, Microsoft Authenticator
Notification	“Approve login?” alert
Biometrics	Fingerprint or Face Identification

6.2 Regular Security Audits: When suspicious, malicious, or policy-violating activity is discovered, security tools, systems, or monitoring platforms create a security alert. Frequent security warnings assist companies in promptly identifying and addressing dangers.

Example:
1. Malware Detection Alerts
2. Unauthorized Login Alerts
3. Network Intrusion Alerts
4. Data Breach Alerts
5. Vulnerability Alerts
6. Phishing Alerts

6.3 Employee Awareness Training: A cybersecurity program called Employee Awareness Training aims to inform staff members on company security rules, safe online conduct, and security risks. Employees that receive training are better able to identify and stop cyberattacks since human error frequently results in security issues. It assists employees in identifying cyberthreats and adhering to security procedures.
6.3.1. The following subjects can serve as the basis for awareness training

1. Phishing awareness includes identifying dubious emails, links, and attachments, confirming the identity of the sender, and reporting phishing attempts.
2. Password security includes using password managers, making strong, one-of-a-kind passwords, and realizing the significance of multi-factor authentication (MFA).
3. Identifying the manipulative techniques employed by attackers and preventing the leaking of private information to unapproved parties are examples of social engineering.
4. Safe Internet and email usage includes handling email attachments properly, avoiding harmful websites and downloads, and browsing securely.
5. Data protection includes understanding data privacy rules, exchanging and storing confidential data appropriately, and disposing of sensitive information securely.
6. Securing laptops and mobile devices, utilizing secure Wi-Fi and VPN connections, and safeguarding company data when working remotely are all examples of mobile and remote work security.
7. Identifying indicators of a security event and being aware of when and how to report suspicious activity are examples of incident reporting.
8. Encryption is the process of applying a mathematical algorithm and an encryption key to transform readable data (plaintext) into an unreadable one (ciphertext). The data can only be decrypted and read by authorized individuals who have the right

key. Because it conceals information and upholds confidentiality, it is crucial for banking and payments.

6.4 Firewalls and intrusion detection systems: monitor and block unauthorized access.
6.4.1 Types of firewalls used in banks

1. Firewall with Packet Filtering Analyzes packets according to their source and destination IP addresses and ports. Traffic is either permitted or prohibited based on regulations.
2. Firewall for Stateful Inspection Only authorized traffic is allowed, and active connections are tracked. More secure than simple packet filtering
3. Firewall for Applications keeps an eye on traffic at the application layer. Prevents SQL injection attacks on banking web apps.
4. Firewall of the Future Generation (NGFW) · Integrates sophisticated threat detection with conventional firewall features. comprises application awareness, malware protection, and deep packet inspection.

6.5 Security information and event management (SIEM): detects and responds to suspicious activities.
6.5.1 Importance of SIEM in banking
Banks manage financial transactions, digital payment systems, and sensitive client data. SIEM aids in safeguarding these resources by:

- Real-time cyberattack detection.
- Tracking system and user activity.
- Recognizing fraudulent transactions.
- Supporting regulatory compliance requirements. • Enhancing the capacity for incident response. • Lowering the possibility of data breaches.

VII. EMERGING TECHNOLOGIES IN BANKING

7.1. Artificial Intelligence (AI): AI enables banks to quickly identify and address security risks.
7.1.1 Applications:

- Fraud prevention and detection
- Verification of customers
- Analysis of behaviour • Information about threats
- Automated reaction to incidents

7.2. Machine Learning (ML): ML allows systems to recognize suspicious activity by learning from past data.
7.2.1 Applications:

- Monitoring transactions
- The identification of fraud
- Evaluation of risk Malware identification
- Advantages of anomaly detection
- Monitoring security in real time Adaptive threat identification
- A decrease in false alarms

7.3. Biometric Authentication: Using distinctive bodily traits, biometric technologies confirm the identities of customers.
7.3.1. Methods:

- Identification of fingerprints
- Recognition of faces
- Scanning the iris
- Voice identification

7.4. Encryption Technology: By transforming data into unintelligible formats, encryption safeguards sensitive information.
7.4.1. Applications:

- Banking transactions conducted online
- Storage of customer data
- Interaction between banking systems

7.5. Blockchain Technology: Blockchain offers a transparent and safe way to record transactions.
7.5.1 Applications:

- Safe transactions
- Verification of digital identities
- Auditing transactions

7.6 Cloud Security Technologies: Cloud computing is used by many banks for services and data storage.
7.6.1 Security Protocols:

- Management of identity and access Benefits of ongoing monitoring
- Safe cloud operations
- Encrypting data
- Enhanced scalability
- Economical security administration

Modern technology is essential to bolstering banking security mechanisms. Multiple levels of defence against cyber threats and financial fraud are offered by technologies such artificial intelligence, machine learning, biometric identification, encryption, fire-

walls, IDS/IPS, SIEM, blockchain, and cloud security. Banks may increase operational resilience, secure transactions, protect client data, and uphold confidence in digital financial services by incorporating this cutting-edge technology. Adoption of contemporary security solutions will continue to be crucial for secure banking operations in the future as cyber threats continue to change.

VIII. CONCLUSION

Modern banking systems, which rely more and more on digital technologies like online banking, mobile apps, ATMs, and cloud-based services, depend heavily on cyber security. Because the banking industry handles a lot of sensitive client data and financial activities, it has become a prominent target for hackers as it continues to evolve. The necessity for robust and dependable security measures is highlighted by threats including phishing, malware, ransomware, data breaches, identity theft, and ATM fraud. Banks use a variety of security measures, such as firewalls, encryption, intrusion detection and prevention systems (IDS/IPS), Security Information and Event Management (SIEM), multi-factor authentication, and ongoing network monitoring, to address these issues. Together, these technologies guarantee the availability, security, and integrity of banking data and services
Additionally, cutting-edge technologies like machine learning (ML) and artificial intelligence (AI) have greatly enhanced banks' capacity to identify and stop cyberthreats in real-time. These technologies improve the adaptability and intelligence of financial systems by aiding in risk assessment, behavioral analysis, fraud detection, and predictive threat intelligence.

REFERENCE

[1] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., and Hur, J., “Cybersecurity threats in FinTech: A systematic review,” Expert Systems with Applications, vol. 241, Art. no. 122697, 2024, doi: 10.1016/j.eswa.2023.122697.

[2] Munira, M. S. K. K., et al., “Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review,” SSRN, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5229868

[3] Mane, P., and Sharma, S. K., “Securing financial transactions: A taxonomical review of cybersecurity strategies in banking,” Business, Management and Economics: Research Progress, vol. 7, 2023, doi: 10.9734/bpi/bmerp/v7/2862.

[4] Ubaldo, A. L. V., et al., “Information security in the banking sector: A systematic literature review on current trends, issues, and challenges,” International Journal of Safety and Security Engineering, vol. 13, no. 1, pp. 97–106, 2023, doi: 10.18280/ijsse.130111.

[5] Ahmad, I., Iqbal, S., Jamil, S., and Kamran, M., “A systematic literature review of e-banking frauds: Current scenario and security techniques,” Linguistica Antverpiensia, 2021. [Online]. Available: https://www.researchgate.net/publication/352668394

[6] Tran, T. N., “Systematic review of cybersecurity in banking: Evolution from pre-Industry 4.0 to post-Industry 4.0,” arXiv preprint, arXiv:2503.00070, 2025. [Online]. Available: https://arxiv.org/abs/2503.00070

[7] Waliullah, M., et al., “Cybersecurity threats and risks in digital banking systems: Systematic literature review,” arXiv preprint, arXiv:2503.22710, 2025. [Online]. Available: https://arxiv.org/abs/2503.22710