International Journal of Cybersecurity Engineering and Innovation

ARTICLE INFO

Article History: Received: 24-11-2025, Revised: 20-12-2025, Accepted: 08-01-2026, Published: 09-01-2026
Corresponding author Email: m_almaiah@ju.edu.jo
DOI:

Volume 2025. No.1

International Journal of Cybersecurity Engineering and Innovation

Innovation and Technology Academic Press

ITAP

Vol. 2026 No.1

Cyber security risk assessment for determining threats and countermeasures for banking systems

Aya Yassin[1], Mohammed Almaayah[1*]
King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan

Abstract

As digital banking services continue to expand rapidly, banking systems have become prime targets for increasingly sophisticated cyber threats. This study presents a comprehensive cybersecurity risk assessment of modern banking systems through the analysis of ten peer-reviewed studies published between 2021 and 2025. The assessment identifies major threats including phishing, malware, distributed denial-of-service (DDoS) attacks, insider threats, and ATM fraud and classifies the key vulnerabilities they exploit, such as weak authentication mechanisms, outdated software, insecure system integrations, and inadequate endpoint protection. Furthermore, the study highlights a range of technical and organizational countermeasures, including multi-factor authentication (MFA), regular patch management, anomaly detection techniques, and user awareness training programs. A structured mapping between threats, vulnerabilities, and corresponding countermeasures is provided to support effective risk mitigation strategies. The findings underscore the critical need for layered security defenses, proactive monitoring, and continuous risk assessment to enhance cybersecurity resilience in the banking sector.

Keywords: Cyber security, Risk Assessment, Threats, Attacks, Countermeasures, multi-factor authentication (MFA).

1. Introduction

In recent years, online banking has transformed the financial industry by offering customers convenient and efficient ways to manage their finances remotely. From checking account balances to transferring funds and making payments, online banking has become integral to daily financial activities. According to industry reports, over 60% of bank customers globally now rely on digital banking channels, highlighting the rapid adoption and growth of online banking services. However, this digital shift has simultaneously expanded the threat landscape, exposing banking systems to a wide range of cyberattacks that can cause financial loss, reputational damage, and regulatory penalties. According to the study by [1], phishing, malware, and man-in-the-middle (MITM) attacks remain the most prominent threats targeting online banking systems. These attacks often exploit weak authentication mechanisms, insecure communication channels, and unprotected user devices, allowing cybercriminals to intercept credentials, hijack user sessions, or implant malicious software into financial systems. Another emerging threat is insider misuse, where bank employees or contractors exploit their legitimate access to compromise sensitive data intentionally or unintentionally. These vulnerabilities are amplified in developing countries, where banks may rely on legacy infrastructure or have limited cybersecurity awareness among users [2].

Effective risk management has therefore become essential for banks to identify, evaluate, and mitigate threats before they lead to significant damage. A structured risk assessment process helps financial institutions uncover system weaknesses, prioritize risks based on potential impact, and implement targeted countermeasures to safeguard operations. As highlighted by multiple studies, the absence of robust security practices—such as encryption, multi-factor authentication, and real-time threat detection—can leave banking systems vulnerable to advanced persistent threats (APTs) and large-scale data breaches. Moreover, the growing sophistication of cybercriminals demands a proactive and adaptive approach to risk assessment and mitigation.

The primary objective of this research is to explore and assess the cybersecurity risks associated with modern banking systems by analyzing ten peer-reviewed research papers published between 2021 and 2025. Through the classification of major threats, system vulnerabilities, and existing security countermeasures, this study aims to establish a clear mapping between the risks and their mitigations. By synthesizing the insights from academic literature, the report will offer a comprehensive view of the current cybersecurity posture in banking and suggest recommendations for improving risk management strategies in this critical domain.

2. Related works

Several studies have been conducted to identify and classify cyber threats in the banking and financial sectors. For instance, Jimmy [1] analyzed in his study the major cybersecurity threats targeting online banking systems, such as phishing, malware, and DDoS attacks. It highlights key vulnerabilities including weak authentication and outdated systems, and proposes countermeasures like multi-factor authentication and encryption. The study emphasizes the need for continuous innovation to combat evolving cyber threats. Darem et al., [2] provided a detailed classification of cyber threats in the banking sector based on severity and technicality, aiming to enhance risk assessment and response strategies. It examines technical, organizational, and legal countermeasures used to protect financial systems. The study also highlights the evolving nature of threats and the challenges in maintaining up-to-date cybersecurity defenses. Oyewole et al., [3] introduced an integrated risk management framework tailored for online banking systems to address security and privacy challenges. It includes threat modeling, vulnerability analysis, and risk quantification to guide mitigation strategies. The framework’s effectiveness is evaluated for real-world implementation and regulatory compliance. Azura et al., [4] reviewed the main common cyber threats to banking systems, with a focus on infrastructure vulnerabilities and malware as the most prevalent threat. It highlights the importance of information sharing and best practices by card issuers and users as key mitigation strategies. The study also discusses proposed models to reduce unmitigated risks in the financial sector. Oyeniyi et al., [5] this study explored the impact of cyber-attacks on financial institutions and their potential consequences on the global economy. It analyzes common attack methods, the effects of COVID-19, and large-scale threats. The study also reviews cybersecurity strategies and considers Distributed Ledger Technology (DLT) as a possible defense solution

In addition, Schreiber and Waismel-Manor [6], they explored data privacy and cybersecurity challenges in banks adopting advanced technologies like AI and blockchain. Through interviews with IT specialists, it identifies key risks such as legacy system integration and vendor management. Strategies include access controls, threat monitoring, and regulatory compliance to maintain security and customer trust. Jaya Sakti et al., [7] discussed evolving cyber threats in banking, including ransomware, phishing, and DDoS attacks, supported by real-world case studies. It identifies vulnerable areas in banking systems and suggests improvements to cybersecurity protocols. The study serves as a guide for researchers and professionals in financial cybersecurity. Shokouhyar et al., [8] reviewed several articles to analyze cybersecurity threats in digital banking, highlighting phishing and malware as the most common. It evaluates countermeasures such as MFA, AI-driven fraud detection, and blockchain, and stresses the importance of regulatory compliance. A multi-layered strategy is recommended to strengthen digital banking resilience. Budiraharjo et al., [9] this study emphasized the importance of intruder detection in cloud-based banking systems and proposes enhanced biometric security measures. It introduces a Smart Online Banking System (SOBS) model using biometric prints and digital signatures to secure transactions. Machine learning and hybrid methods are employed to improve threat detection and data protection. Maditinos et al., [10] analyzed the cybersecurity landscape in the banking sector amid growing digital transformation and cybercrime. It assesses current frameworks and proposes adaptive strategies using AI, big data, and continuous risk assessment. The study emphasizes the need for a holistic approach to strengthen cybersecurity resilience and protect customer trust.

3. Methodology

This section presents the main stages of the study, which are structured based on a risk assessment framework applied to banking systems. The framework is built upon findings from ten research papers published after 2021. It aims to systematically identify and classify the main threats, vulnerabilities, and countermeasures, as well as map the relationships between them. Each step of this framework contributes to building a clear and comprehensive picture of the cybersecurity risk landscape in modern banking environments. Figure 1 shows the research methodology steps for this study.

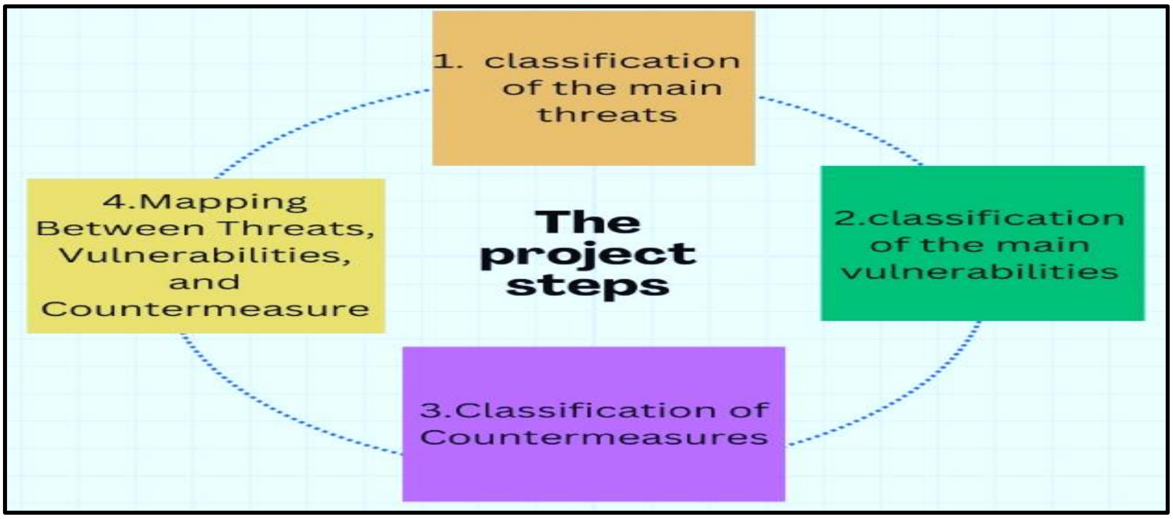
1. classification of the main threats
2.classification of the main vulnerabilities
3.Classification of Countermeasures
4.Mapping Between Threats, Vulnerabilities, and Countermeasure
The project steps

Figure 1. Research Methodology

3.1 Step One: Classification of the Main Threats

The first step in the framework focuses on identifying and classifying the most common cybersecurity threats that target banking systems. This process was carried out by analyzing the selected research papers and extracting detailed information about real-world attacks, their techniques, and behaviors. These threats include phishing attacks, malware infections, Distributed Denial-of-Service (DDoS) attacks, man-in-the-middle (MITM) attacks, and insider threats. Each threat was linked to a specific part of the banking infrastructure, such as the user interface, transaction layer, communication channels, or internal systems. The classification process was guided by three main criteria: the type of the threat, its operational context (place of threat), and its potential impact on confidentiality, integrity, and availability (CIA) of banking services.

3.2 Step Two: Classification of the Main Vulnerabilities

In the second step, the framework addresses the identification and classification of key vulnerabilities that exist in banking systems. Vulnerabilities are weaknesses in the system that could be exploited by cybercriminals to carry out attacks. Through an extensive review of the selected literature, several common vulnerabilities were identified, such as weak password policies, absence of multi-factor authentication, outdated software components, improper input validation in banking apps, and insecure communication protocols. Each vulnerability was categorized according to its location in the system (e.g., user authentication layer, application layer, or data layer), its technical nature, and the risk it poses. This step helps reveal the internal weaknesses that make banking systems susceptible to various threats.

3.3 Step Three: Classification of Countermeasures

The third step involves identifying and classifying the security countermeasures proposed in the literature to address the threats and vulnerabilities identified in the previous steps. Countermeasures include technical, procedural, and organizational controls that aim to reduce the risk or impact of attacks. Examples include implementing strong encryption protocols (e.g., TLS/SSL), deploying multi-factor authentication (MFA), using intrusion detection systems (IDS), and enforcing access control mechanisms such as Role-Based Access Control (RBAC). This classification highlights which countermeasures are most effective for specific types of threats or system weaknesses. The data collected in this step supports the creation of a practical defense strategy tailored for banking systems.

3.4 Step Four: Mapping Between Threats, Vulnerabilities, and Countermeasures

The final step in the framework establishes a clear mapping between the threats, vulnerabilities, and countermeasures analyzed in the previous steps. By linking each threat to its corresponding vulnerability and associated countermeasure, the study provides a structured view of how attacks occur and how they can be mitigated. This mapping also helps identify gaps where specific threats do not yet have adequate controls or where vulnerabilities are left unprotected. The outcome of this step contributes to building a more resilient banking security model that aligns with risk management best practices.

4. Classification of the Main Threats

This section presents the classification of the main cybersecurity threats targeting banking systems, based on the analysis of ten peer-reviewed research papers published after 2021. Each threat is categorized according to its type, place of occurrence within the system.

Table 1. Classification of the Main Threats

Type of threat	Place of threat	Description of threat	Impact of threat
Phishing Attacks(1)	Login portal – email links(1)	This is a criminal crime involving social engineering and technology to get sensitive information from an Internet user. Phishing strategies use a variety of communication channels, including email, instant chats, pop-up messages, and Web .(9)	Financial loss, loss of user trust(1)
DDoS Attacks(1)	Network/Infrastructure layer(9)	Overloads a bank's servers with traffic to render the platform unusable.(1)	Service disruption, loss of availability, customer dissatisfaction(9)
Malware (2)	Endpoint devices / User systems	Malicious software designed to compromise damage or gain unauthorized access to computer systems or networks.(2)	Data theft, system compromise, financial loss
Man-in-the Middle (MitM) (2)	Network communication layer	Attackers intercept communications to steal data or alter transactions.(1)	Session hijacking, data leakage
Advanced Persistent Threats (2)	Entire banking infrastructure	Sophisticated, often state-sponsored, cyberattacks that persist undetected for an extended period of time. Focus on stealing specific sensitive information from the target organization.(2)	Data breaches, espionage, large-scale damage
Distribute d Denial of Service(2)	Network/Server layer	Overwhelming target system or network with traffic, rendering it inaccessible or unusable.(2)	Downtime, service unavailability, loss of customer trust

Cryptocurrency related Threats (2)	Online transaction and exchange layers	Cyber threats targeting the theft or manipulation of digital currencies, wallets, or exchanges.(2)	Loss of digital assets, fraud
Buffer overflow (3)	Application backend	By overwriting some of the application's memory, attackers take advantage of buffer overflow flaws to change the route of execution. The malicious data can include code that is intended to set off particular events, thereby delivering the attacked program new instructions that might lead to unauthorized access to the system (3)	Unauthorized access, system crashes
Injection (3)	Database / Input forms	Injection can occur in different aspects including browsers or Structured Query Language (SQL) when malicious code is being inserted into servers(3)	Data leaks, unauthorized access to accounts
Sniffing (3)	Network transmission	The process of intercepting communication or directing it toward a destination so that it may be recorded, examined, and kept track of. Attackers may intercept and read any network packet containing plain-text data. Usernames, passwords, secret phrases, financial information, or any other information that the attacker might find valuable can be obtained to launch further attacks	Data exposure, identity theft
ATM - machine fraud (4)	Physical layer / ATM hardware	Use of skimming devices or fake ATMs to steal card information	Direct financial theft, identity compromise
Identify theft (4)	Across systems (web, mobile, ATM)	This type of cyberattacks involves the theft of another person's personal or financial information in order to commit fraud in their name. Its victims are usually left with credit, financial, and reputational loss.	Account takeover, fraud
Virus And Trojans (7)	User devices / internal network	Malicious code disguised as legitimate software that compromises banking systems	Information theft, system damage

Credit Card Fraud (7)	Online payment platforms	Unauthorized use of stolen card data in transactions	Financial losses, legal consequences
Insider Threats (2)	Internal employee access	Authorized personnel abuse their access rights for malicious purposes	Data tampering, breaches, loss of trust
Credential Stuffing Attacks[6]	Online Banking Systems	Exploiting stolen credentials from previous breaches to gain unauthorized access to bank accounts.	Unauthorized access to user accounts and financial loss.
Business Email Compromise (BEC) [6]	Internal Communication Channels	Impersonating executives or trusted partners via email to deceive employees and steal funds or data.	Financial theft and leakage of sensitive internal data.
ATM Malware Attacks [6]	ATM Infrastructure	Installing malware on ATMs to withdraw cash or harvest card data.	Loss of funds and customer data compromise.
Mobile Banking Trojans [6]	Mobile Banking Applications	Malware targeting mobile banking apps to steal login credentials and perform unauthorized transactions.	Loss of customer funds and sensitive data exposure.
Fake Banking Apps[6]	Mobile App Stores / User Devices	Deceptive apps designed to mimic legitimate banking applications to trick users into sharing sensitive data.	Mass credential theft and reputational damage to banks.

1. Phishing Attacks

Definition: Phishing attacks use deceptive emails, messages, or websites to trick users into providing sensitive information, such as login credentials or credit card numbers.

Mechanism: Attackers often impersonate a trusted entity, such as a bank or government authority, to gain users' trust. These messages may include links to fraudulent websites resembling legitimate banking portals, where users unknowingly enter their credentials, giving attackers direct access to their accounts.

Impact on Online Banking: Phishing is one of the leading causes of financial fraud in online banking, accounting for billions in losses worldwide. Beyond financial theft, phishing compromises user trust, affecting the bank's reputation and customer loyalty.

Real-world Example: The COVID-19 pandemic saw a sharp increase in phishing scams targeting online banking users, with messages claiming to provide relief information or urgent updates.

2. Man-in-the-Middle (MitM) Attacks

Definition: A MitM attack occurs when an attacker intercepts the communication between a user and a bank's server, allowing them to eavesdrop on or alter the information being exchanged.

Mechanism: Attackers typically exploit unsecured or weakly secured network connections, like public Wi-Fi, to intercept data. By placing themselves between the user and the bank, they can redirect funds, alter transaction details, or steal login credentials.

Impact on Online Banking: MitM attacks undermine the integrity of data, leading to financial theft or unauthorized account access. They also compromise user trust in digital banking platforms, as users may feel vulnerable even on seemingly secure connections.

Real-world Example: Attackers often create fake public Wi-Fi hotspots mimicking trusted networks. Once connected, any data the user transmits, such as login details, can be intercepted by the attacker.

5. Classification of the Main Vulnerabilities

The following table presents the main vulnerabilities identified in banking systems based on the reviewed literature. These vulnerabilities represent technical weaknesses or misconfigurations that could be exploited by cyber attackers to compromise confidentiality, integrity, or availability. Each entry is classified according to the type of vulnerability, where it occurs within the system, its technical description, and its potential impact.

Table 2. Classification of the Main Vulnerabilities

Type of vulnerabilities	Place of vulnerabilities	description of vulnerabilities	Impact of vulnerabilities
Weak Authentication (1)	Login/authentication system	Easily guessable or phish able credentials.	Unauthorized access, fraud, data breaches
Insecure Network Connections (1)	Communication layer	Lack of encryption on public or unsecured connections	Data interception, fraud, data breaches
Outdated software and systems (1)	Application and infrastructure layer	Vulnerabilities in unpatched or legacy systems	Data breaches, system compromise , operational disruption
Third party integration (1)	External services / APIs	Dependencies on third party services with weak security	Data exposure , supply chain attacks , regulatory issues

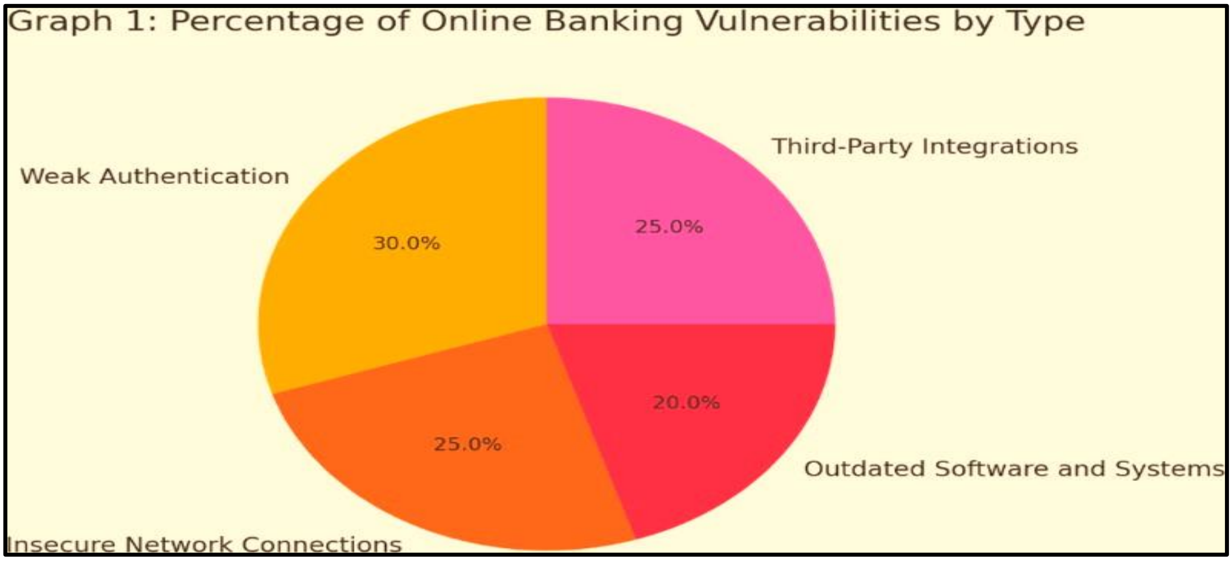

Figure 2. Types of Vulnerabilities in online banking system.

Table 3. Classification of the Main Vulnerabilities

Type of vulnerabilities	Place of vulnerabilities	description of vulnerabilities	Impact of vulnerabilities
Weak cryptography algorithms (3)	Encryption module	Inappropriate cyphers such as short key lengths, shoddy encryption techniques, and careless key handling are examples of poorly constructed cryptographic methods	Enables attackers to decrypt sensitive data
Unpatched known vulnerabilities (3)	System and application layer	Neglected flaws may become a preferred entry point for malicious actors to compromise networks and perform ransomware attacks	Increases chances of successful exploitation

Obsolete, unsupported or unapproved components (3)	System architecture	These components are not covered by proper security updates and patches that can shield users from known vulnerabilities	Introduces unmonitored and vulnerable elements
Improper certificate validation (3)	Transport layer (TLS/SSL)	A certificate is either not validated by the system or is validated erroneously. An attacker may be able to impersonate a trusted entity by interfering with the communication between the host and client when a certificate is malicious or incorrect	Enables MITM and spoofing attacks
Missing CAPTCHA protection in URLs (3)	Web application interface	Sending a specially crafted request to the web interface would allow an attacker to take advantage of this weakness. A successful vulnerability could enable the attacker to determine the validity of a username and the user’s identity	Leads to automated attacks like credential stuffing
Improper generation and protection of session identifier token(3)	Session management	Session ID should not be re- used or predictable to attackers. Any transfer of the value must be encrypted as regarded as sensitive data	Allows session hijacking and impersonation
Improper restriction of invalid sessions(3)	Session management	Sessions fail to be invalidated when users quit the browsers without logging out, or both session objects on the server and the session identifier cookie on the client browser have not been rendered	Can be reused by attackers to gain unauthorized access

		invalid	
Inadequate detection of insider threats (2)	Internal network / access controls	No monitoring or alerts for suspicious behavior from employees	Leads to unauthorized actions and data leaks
No runtime threat re-evaluation(9)	Security monitoring system	The system fails to reassess threats dynamically	Leaves the system vulnerable to evolving attack methods
Lack of multi-factor authentication (MFA) (7)	User authentication layer	Systems lack additional verification beyond passwords	Increases risk of credential-based attacks
Weak endpoint protection (7)	User devices / client layer	No antivirus or real-time protection on user endpoints	Allows malware infections and data loss
SQL injection weakness(7)	Database interaction layer	User input is not properly sanitized before reaching the database	Attackers can manipulate or extract data from databases

6. Classification of Countermeasures

Technical countermeasures are tools and techniques designed to protect systems and data from cyber threats. They are essential for safeguarding the integrity of information systems, and cyberattacks. They can networks, and data from unauthorized access dimensions based on their primary functions be classified into several and use cases. Table 4 outlines the primary security countermeasures proposed in the literature to mitigate the identified threats and vulnerabilities in banking systems. Each countermeasure is classified based on its type, the system layer where it is applied, a brief explanation of how it works, and the expected impact on improving system security.

Table 4. Classification of the Main Countermeasures.

Type of countermeasures	Place of countermeasures	description of countermeasures	Impact of countermeasures
Encryption (2)	Data storage & transmission	Banks use encryption to protect sensitive data, both in transit and at rest. Encryption ensures that data can only be accessed and read by authorized individuals, preventing unauthorized access and data breaches.	Prevents unauthorized data access and tampering

Multi-factor Authentication(MFA) (2)	User login / access control	MFA requires users to provide multiple forms of identification before accessing sensitive systems or data. This can include passwords, biometrics, or hardware tokens, making it more difficult for attackers to gain unauthorized access using stolen credentials.	Reduces risk of credential theft and account compromise
Network Segmentation (2)	Internal network infrastructure	Network segmentation involves separating different parts of the network to limit unauthorized access and the potential spread of an attack.	Contains breaches and minimizes lateral movement
Firewall and Intrusion Prevention Systems (IPS) **(2)**	Network perimeter	Firewalls and IPS protect the internal network of banks from unauthorized access and intrusion attempts. They monitor incoming and outgoing network traffic, blocking malicious activity, and preventing unauthorized access to sensitive data.	Stops intrusion attempts and detects known attacks
Regular Security Patching (2)	System and application layers	Banks must keep their systems and software up- to-date by applying security patches and updates regularly. This helps to close known vulnerabilities that attackers could exploit.	Closes security gaps before exploitation occurs
Endpoint Security(2)	User devices (PCs, mobiles)	Implementing endpoint security solutions, such as antivirus and antimalware software, helps protect individual devices from threats	Prevents malware infection and data exfiltration

		like malware, ransomware, and targeted attacks.	
Security Information and Event Management (SIEM)(2)	Security operations center (SOC)	SIEM systems collect, analyze, and correlate data from various sources to detect and respond to potential security incidents. They provide real-time monitoring and alerts, enabling banks to respond quickly to cyber threats.	Enables fast incident detection and response
Data Loss Prevention (DLP) tools [2]	Data access & sharing controls	DLP tools monitor and prevent the unauthorized transmission of sensitive data, both within and outside the organization.	Prevents data leakage and insider threats
Encrypted Communication **(2)**	Communication channels	Using encrypted communication channels, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), protects sensitive data in transit and prevents unauthorized access or interception.	Secures communications against eavesdropping (MitM)

7. Mapping between the threats, vulnerabilities and countermeasures

To develop an effective cybersecurity risk management strategy for banking systems, it is essential to understand the relationships between threats, the vulnerabilities they exploit, and the countermeasures that can mitigate them. The following table provides a comprehensive mapping that links common threats identified in recent research to their underlying vulnerabilities, and the recommended security controls used to prevent or reduce their impact.

Table 5. Mapping between the threats, vulnerabilities and countermeasures

Type of Threat	Type of Vulnerability	Type of Countermeasure
Phishing Attacks	Weak Authentication	Multi-factor Authentication (MFA)
DDoS Attacks	Insecure Network Connections	Firewall and Intrusion Prevention Systems (IPS)
Malware	Outdated software and systems	Regular Security Patching

Man-in-the Middle (MitM)	Improper certificate validation	Encrypted Communication
Advanced Persistent Threats	No runtime threat re- evaluation	Anomaly Detection
Credential Stuffing Attacks	Weak Authentication	Multi-factor Authentication (MFA)
ATM Malware Attacks	Weak endpoint protection	Endpoint Security
Fake Banking Apps	Obsolete, unsupported or unapproved components	Preventive measures and safety mechanisms
Injection	SQL injection weakness	Firewall and Intrusion Prevention Systems (IPS)
Insider Threats	Inadequate detection of insider threats	Security Information and Event Management (SIEM)
Distribute d Denial of Service	Insecure Network Connections	Network Segmentation
Cryptocurrency related Threats	Weak cryptography algorithms	Encryption
Buffer overflow	Unpatched known vulnerabilities	Regular Security Patching
Sniffing	Improper generation and protection of session identifier token	Deception Technologies
ATM - machine fraud	Weak endpoint protection	Endpoint Security
Identify theft	Weak Authentication	Multi-factor Authentication (MFA)
Virus And Trojans	Unpatched known vulnerabilities	Regular Security Patching
Cradit CardFraud	Lack of multi-factor authentication (MFA)	Multi-factor Authentication (MFA)
Business Email Compromise (BEC)	Third party integration	Cooperative, partially, and integrated model
Mobile Banking Trojans	Improper restriction of invalid sessions	User awareness campaigns

7.1 Percentage of Cyber Threats in Banking Systems

As cyber threats targeting the financial sector continue to rise, understanding their prevalence is crucial for effective risk management and defense planning. The chart below illustrates the distribution of the most common types of cyber-attacks against banking systems, based on recent global cybersecurity studies and incident reports from 2024–2025 as shown in Figure 3. These statistics highlight the critical areas that require prioritized protection and proactive security measures.

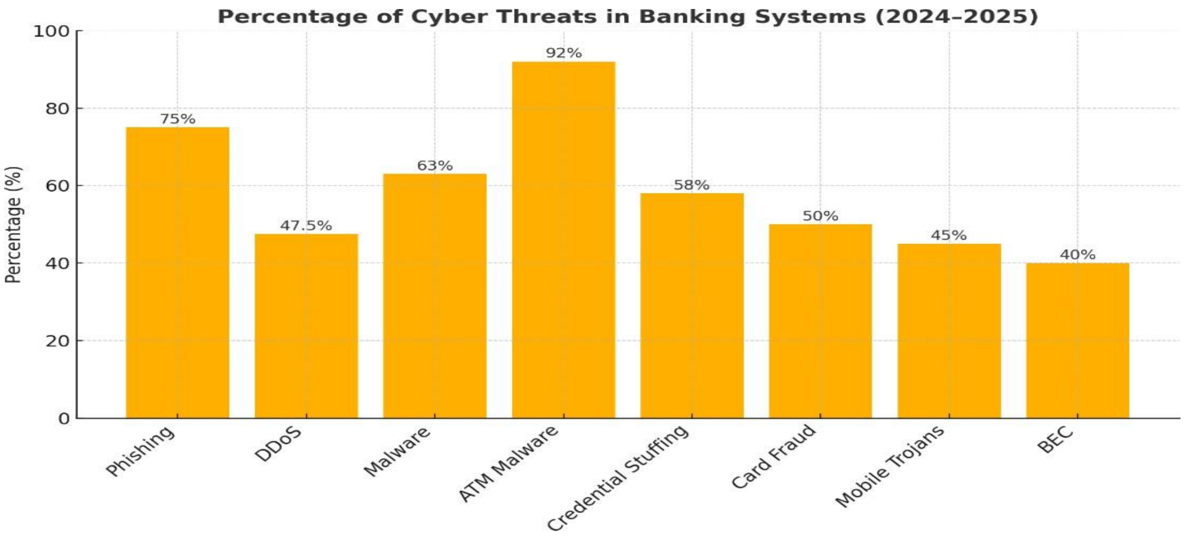

Figure 3. Analysis of cyber threats in banking system (2024-2025).

8. Conclusion

In this research, a comprehensive risk assessment of cybersecurity threats targeting banking systems was conducted. By analyzing recent scholarly literature and real-world security data, several critical threats were identified, including phishing, malware, distributed denial-of-service (DDoS) attacks, ATM fraud, and advanced persistent threats (APTs). These threats exploit a range of vulnerabilities such as weak authentication mechanisms, outdated software, insecure system integrations, and inadequate endpoint protection. By systematically mapping threats to their associated vulnerabilities and corresponding countermeasures, the study provides valuable insights into how financial institutions can strengthen their defenses against evolving cyber risks. The implementation of layered security controls—including multi-factor authentication, regular patch management, encryption, and user awareness training plays a crucial role in minimizing risk exposure. Ultimately, proactive risk management, continuous threat monitoring, and the cultivation of a strong cybersecurity culture are essential to ensuring the resilience, security, and trustworthiness of modern banking systems. This study offers a solid foundation for future research and the practical adoption of cybersecurity best practices in the financial sector.

References

[1] Jimmy, F. (2024). Cybersecurity Threats and Vulnerabilities in Online Banking Systems. International Journal of Scientific Research and Management (IJSRM), 12(10), 1631–1646. https://doi.org/10.18535/ijsrm/v12i10.ec10

[2] Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. IEEe Access, 11, 125138-125158.

[3] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625-643.

[4] Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. Journal of Banking and Financial Technology, 1-20.

[5] Oyeniyi, L. D., Igwe, A. N., Ofodile, O. C., & Paul-Mikki, C. (2021). Optimizing risk management frameworks in banking: Strategies to enhance compliance and profitability amid regulatory challenges. Journal name missing.

[6] Schreiber, A., & Waismel-Manor, I. (2024). Cyber risk assessment model for information assets: a tailored approach for the financial and banking sector. Journal of Operational Risk.

[7] Jaya Sakti, M. A., Achsani, N. A., & Syarifuddin, F. (2018). Online banking implementation: Risk mapping using erm approach. Bulletin of Monetary Economics and Banking, 20(3), 279-306.

[8] Shokouhyar, S., Panahifar, F., Karimisefat, A., & Nezafatbakhsh, M. (2018). An information system risk assessment model: a case study in online banking system. International Journal of Electronic Security and Digital Forensics, 10(1), 39-60.

[9] Budiraharjo, R., Silhi, A. J. R., & Prihartono, N. I. G. A Risk Management Guide for Information System Infrastructure in Digital Banking. information technology, 22, 23.

[10] Maditinos, D., Chatzoudes, D., & Sarigiannidis, L. (2013). An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk. Journal of Systems and information Technology, 15(1), 97-116.