STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

JOURNAL OF CYBER SECURITY AND RISK AUDITING
Smart Technologies Academic Press
STAP

A Systematic Review of Security Risk Management for Banking Systems

Aitizaz Ali[1], Rami Shehab[2]

[1] *School of Technology, Asia Pacific University of Technology and Innovations, Kuala Lumpur, Malaysia*

[2] *Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

ARTICLE INFO

Article History

Received: **07-06-2023**
Revised: **22-07-2023**
Accepted: **02-08-2023**
Published: **04-08-2023**

Vol.2023, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2023.1.4

Corresponding author.
Email:
rtshehab@kfu.edu.sa

Orcid:

https://orcid.org/0000-0002-1537-4932

ABSTRACT

This study investigates the critical and recent threats and vulnerabilities of the last three years, from 2021 to 2024. The main objective of this article is to discuss the main threats and vulnerabilities facing banking institutions and analyzing these risks and their impact, the main countermeasures and security controls in banking, while interpreting risk management strategies including: identifying, assessing, and mitigating potential risks. This study also analyzes threats, vulnerabilities, and countermeasures in banking field. This work presents a systematic approach to highlight and assess potential vulnerabilities and threats in the banking systems. By understanding threats, vulnerabilities, and countermeasures developers and defenders can anticipate threats and attacks, take measures against them, and completely mitigate them.

Keywords: Banking systems, Cybersecurity, Threats, Vulnerabilities, Cyber-attacks, and Countermeasures.

How to cite the article

Ali, A., & Shehab, R. (2023). A Systematic Review of Security Risk Management for Banking Systems. Journal of Cyber Security and Risk Auditing, 2023(1), 49–72. https://doi.org/10.63180/jcsra.thestap.2023.1.4

1. Introduction

The increasing use of online banking, mobile banking, and other digital services has made it easier for criminals to exploit weaknesses in systems [1]. Therefore, banks and financial institutions face several security challenges and cyberattacks such as phishing and DDoS attacks, data breaches and ransomware incidents [2]. Cyber threats in the banking sector can have a significant impact, including financial loss, reputation damage, and legal consequences also posing risks to the stability and integrity to these institutions [3]. Hence, financial institutions must develop and implement effective risk management strategies [4][5]. The growing number and impact of cyber-attacks on banking information system represents a critical international security threat. Banking sector systems face security risks from sophisticated threat on a several forms such as worms, malware, ransomware and others. Across pivotal sectors like banking and financial systems, vulnerabilities are growing as systems become more interconnected and dependent on data.

Several attacks target banking sector platforms and services such as payment systems and mobile banking applications in order to collect sensitive information and credentials and then execute illegitimate operations. Several types of vulnerabilities have been exploited by attackers such as update failure, fake calls mimicking Trojans, software defects and others. [11] These threats aim to theft data or information of users, their money, monitor the financial activities of specific target customers and tampering the financial services. Nevertheless, as these banking systems become more depending on smart technologies and smart networks, they also become more vulnerable to cyber-attacks [4]. Banking systems have many vulnerabilities, due to their poor design of architectures, weak security mechanisms, and implemented cryptographic primitives, that can create opportunities for attackers to gain access to or control over the system and achieve their intended malicious purposes [5]. Thus, any possible disruption in the banking systems has a great impact on financial sectors and thus failure.

Cybersecurity risk management involves identifying and mitigating risks associated with cyber threats [6]. This includes adopting advanced security technologies and educating employees on good security practices while staying up to date with the latest threats [7]. Some of the reasons that make Risk management and risk assessment crucial are: Protecting Financial Stability, Protecting Reputation and customers trust, the sensitivity of the data these institutions hold, balance technological advancement with risk mitigation [8][9][10].

Various papers have investigated the vulnerabilities and threats of banking systems from different perspectives. This study investigates recent threats and vulnerabilities of the last three years, from 2021 to 2024. The main objective of this article is to discuss the main threats and vulnerabilities facing banking institutions and analyzing these risks and their impact, the main countermeasures and security controls in banking, while interpreting risk management strategies including: identifying, assessing, and mitigating potential risks. This study also analyzes threats, vulnerabilities, and countermeasures in banking field. This work presents a systematic approach to highlight and assess potential vulnerabilities and threats in the banking systems. By understanding threats, vulnerabilities, and countermeasures developers and defenders can anticipate threats and attacks, take measures against them, and completely mitigate them.

2. Related works

Various papers have investigated the vulnerabilities and threats of banking systems from different perspectives. For instance, Darem et al., [1] in their study on cyber threats Classifications and countermeasures in banking and financial sector in 2023. The paper discusses various cyber threats in the banking sector, such as unauthorized access and data breach. It proposes security models such as biometric authentication and machine learning-based security system to protect sensitive data. The research focuses on the importance of proactive measures such as intrusion detection to reduce risks in online banking systems. Kristian et al., [2] conducted a study for enhancing cybersecurity risk management strategies in financial institutions through a comprehensive analysis of threats and mitigation approaches. The article discusses the growing cyber threats facing financial institutions, such as phishing, malware, and data breaches. It suggests strategies to improve cybersecurity management, such as the use of advanced technologies, employee training, and effective incident response plans. It also highlights the importance of regulatory frameworks and preventive assessments to help effectively mitigate these threats.

Lavanya and Mangayarkarasi [3] performed a review study on detection of cybersecurity threats in banking sectors using Ai based risk assessment. The article reviewed the continuous increase in cyber threats in the banking sector, and how advanced attacks affect financial institutions. It is proposed to use artificial intelligence to assess risks and improve security systems to detect and mitigate threats. It also discusses common attacks such as ransomware and phishing and urges enhanced security using technologies such as strong passwords, digital certificates (SSL), and virtual private networks (VPN).

A review study by Kamuangu [4] on cybersecurity in fintech to focus on threats, solutions, and future Trends. The article discusses the growing cybersecurity challenges in the fintech sector, including threats such as data breaches and phishing attacks. It also reviews defensive measures such as encryption and multi-factor authentication, as well as emerging solutions such as computer-resistant encryption and behavioral analytics. The research provides valuable insights into the future of fintech security and makes recommendations for addressing current and future cybersecurity risks. Another study by Ghelani et al., [5] namely cyber security threats, vulnerabilities, and security solutions models in banking. The paper discusses various cyber threats in the banking sector, such as unauthorized access and data breach. It proposes security models such as biometric authentication and machine learning-based security system to protect sensitive data. The research focuses on the importance of proactive measures such as intrusion detection to reduce risks in online banking systems. Alkhdour et al., [6] also conducted as assessment study for analyzing cybersecurity risks and threats on banking and financial services. This paper investigates at how technology has changed banking, but also increased cyber risks like malware and security breaches. It explains that sharing information and following best practices can help reduce these risks. However, it also finds that current security measures and laws are not enough to protect financial institutions properly.

Meduri [7] conducted a study on cybersecurity threats in banking through unsupervised fraud detection analysis. This article shows how unsupervised learning can improve fraud detection in banking. It explains how to use it to find unusual patterns and suggests ways to make it even better with advanced machine learning. The goal is to protect digital banking from fraud. Another study by Familoni et al., [8] compared cybersecurity in the financial sectors of the USA and Nigeria. The USA has strong technology and rules but faces complex cyber-attacks. Nigeria has less awareness and technology, and changing regulations. Both countries need to improve cybersecurity by using better technology, stronger rules, more awareness, and working together internationally. Alhashmi et al., [9] performed a quantitative assessment for proposing a cyber risk framework for the financial sector. This paper looks at the growing cyber risks to financial stability, such as data breaches and fraud. It introduces a new method to measure these risks, estimating potential losses for the financial sector between 10% and 30% of net income. Finally, Somogyi and Nagy [10] presented main cyber threats and security challenges in the Hungarian financial sector. The paper examined the rise in cyber-attacks on the banking industry and the importance of information security. It looks at Hungary's financial sector, identifying key services, current cyber threats, and best security practices based on regulations and standards.

Despite several studies have investigated the vulnerabilities and threats of banking systems from different perspectives. This study investigates recent threats and vulnerabilities of the last three years, from 2021 to 2024. The main objective of this article is to discuss the main threats and vulnerabilities facing banking institutions and analyzing these risks and their impact, the main countermeasures and security controls in banking, while interpreting risk management strategies including: identifying, assessing, and mitigating potential risks. This study also analyzes threats, vulnerabilities, and countermeasures in banking field.

3. Analysis and findings

3.1 Findings of classification of threats in banking system

References	Type of threats	Place of threats	Description of threats	Impact of threats
[1]	Phishing Attacks	Banking systems	An attempt to deceive users through fake messages to extract sensitive information	Theft of user Credentials or financial data
	Ransomware	sensitive data	Malicious software that encrypts data and demands ransom for decryption.	Data loss, significant financial payment, and service disruptions
	Distributed Denial of Service (DDoS)	Banking systems	Sending massive requests to disrupt a system,	Service downtime and financial losses due to operational

			making it unable to serve users.	disruptions
	Insider Threats	Banking systems	Harmful actions performed by employees with access to sensitive systems intentionally or unintentionally	Leakage of confidential data, financial loss, and damage to reputation
	Advanced Persistent Threats (APTs)	Banking systems and sensitive data	Long-term attacks using advanced techniques to steal sensitive data.	Theft of financial data and sensitive information causing severe harm
	Social Engineering Attacks	Employees of financial institutions	Deceptive manipulation of individuals to reveal confidential information.	Data breach and loss of sensitive information
	Data Breaches	Banking systems	Unauthorized access to Sensitive information or data.	Exposure of personal and financial data, leading loss reputation
	Malware Attacks	Banking systems, data centers	Malicious software (Excluding ransomware) that disrupts systems and steals data.	System damage, data loss, and potential Financial theft
[2]	Phishing Attacks	Email, Websites	Fraudulent attacks to steal user data	Disrupt banking access, loss of sensitive information
	Ransomware	Banking networks	Encryption software Demanding ransom	Financial loss, Disruption of services
	Distributed Denial of Service (DDoS)	Online banking systems	Overwhelms servers with excessive traffic	Cripples online services, causing service downtime

	Advanced Persistent Threats (APTs)	Financial data systems	Long-term attack to steal or manipulate sensitive data	Loss of financial integrity, regulatory penalties
	Malware Attacks	Internal and external systems	Malicious software Damaging systems/files	Data corruption, downtime in online service
[3]	Phishing	Emails	Hidden emails are used to trick clients into opening links or messages, leading to malware installation on sensitive	Leads to theft of sensitive customer data and compromise of network security
	Ransomware	Banking infrastructure	Ransomware locks files and demands a ransom for decryption	Causes business Interruptions and locks critical banking systems until ransom is paid
	Email Malware	Emails	Malicious links or attachments in emails infect systems with viruses	Sends user Information to hackers and spreads malware across networks
	Mobile Malware	Mobile applications	Malicious mobile apps steal information such as photos videos, and sensitive financial data	Allows hackers to steal One-Time Passwords (OTPs) and execute unauthorized financial transactions
[4]	Data Breach	Financial Platforms	Unauthorized access to sensitive customer data through system vulnerabilities.	Significant financial impact (e.g., $12.5 million in 2020) and increased risks to data security.

	Phishing Attacks	Digital Platforms (Email, Websites)	Using fake messages r websites to deceive victims into disclosing personal information.	47% increase in attacks in 2021 Moderate financial impact ($8.2 million in 2020)
	Malware and Ransomware	Financial Institutions	Inserting malicious software to destroy r encrypt data, demanding a ransom.	Severe financial impact ($15.7 million in 2020) and increased attack complexity.
	loT-based Attacks	Connected Devices in Financial Services	Exploiting vulnerabilities in connected devices to breach financial systems	Potential unauthorized access to financial data, posing a significant threat to privacy.
	Deepfake Technology	Digital and Financial Platforms	Using deepfake technology to manipulate voice or video to convince victims into making fraudulent transactions.	Major threat to financial transactions and security, contributing to the spread of misinformation.
[5]	Denial-of-Service e (DoS)	Banking networks	Prevents users from accessing systems by overwhelming the network with traffic	Causes service outages and disrupts financial transactions.

	Malware	Banking systems and devices	Malicious software exploits vulnerabilities to gain unauthorized access to sensitive information.	Significant financial or political damage by compromising customer data
	Phishing	Customer communications	Social engineering tactics to trick customers into revealing sensitive information like passwords.	Theft of Personal credentials and financial data.
	SQL Injection	Bank databases	Injecting malicious SQL queries to access or manipulate database information illegally.	Leads to unauthorized data access, loss of functionality, and confidentiality breaches.
	Man-in the-Middle (MITM)	Communication channels	Intercepting and manipulating communications between two parties without their knowledge.	Unauthorized data access, altered transactions, and theft of sensitive information.
[6]	Malware Attacks	Banking systems and devices	Include ransomware, phishing, viruses, and worms exploiting vulnerabilities	Leads to financial losses, theft of sensitive data, and service disruptions.

	Phishing	Customer interactions	Fraudulent attempts to trick users into sharing sensitive information like login credentials	Results in identity theft, financial fraud, and reputational damage.
	Distributed Denial of Service (DDoS)	Banking networks	Overloading servers with massive traffic, disrupting operations and access.	Causes system downtime, service unavailability, and customer dissatisfaction
	Data Leakage/ Data Theft	Financial databases	Unauthorized access or transfer of sensitive data to external sources	Compromises Confidential it ,results in Financial losses, and damages trust
	Social Engineering Attacks	Customer and employee communications	Manipulative techniques to exploit human errors and extract critical information.	Facilitates unauthorized access and compromises systems
[7]	Malware	Banking systems and software	Malicious software used to infiltrate systems, steal data, or disrupt operations.	These attacks aim to steal money from victims, tamper with processes, and compromise confidential financial information
	Phishing Attacks	Email or malicious links	Fraudulent attempts to trick users into providing sensitive information through fake messages or websites	These risks put financial organizations and their customers at high risk of identity theft, fraud, and data breaches

	ransomware	Banking systems and digital networks	Attacks that encrypt data and prevent access until a ransom is paid to the attackers.	Ransomware attacks that destroy financial infrastructure
	DDoS (Distributed Denial of Service)	Servers and network infrastructure	Attacks aimed at disrupting services by overwhelming servers with massive amounts of requests, affecting their performance	These attacks aim to steal money from victims, tamper with processes, and compromise confidential financial information
[8]	Malware Attacks	Financial systems And customer devices	Malware infiltrates systems to steal sensitive data, disrupt operations or enable unauthorized access. Delivered through phishing emails or compromised sites.	Malware can enable hackers to exfiltrate sensitive financial information, manipulate transactions, or sabotage critical systems
	Phishing Attacks	Email, SMS, and malicious links	Fraudulent communication aimed at tricking individuals into revealing confidential data, such as login credentials or financial details	Phishing attacks can lead to unauthorized access to online banking accounts, identity theft, and financial fraud
	Distributed Denial of Service (DDoS)	Banking servers and online platforms	Overloads financial servers with excessive traffic, disrupting services like online banking. payment systems and trading platforms.	DDoS attacks...can disrupt online banking services trading platforms and payment processing systems
	insider Threats	Internal banking systems and staff access	Threats originating from employees or contractors who misuse their privileged access to steal data, manipulate systems or sabotage operations.	Insiders may abuse their access privileges to steal sensitive data manipulate financial records, or sabotage systems

[9]	Technologically Induced Vulnerabilities	Digital Banking Systems	Weaknesses caused by technological advancements in banking systems that make them prone to attacks	Finance technologies are more prone to cyberattacks arising from technologically induced vulnerabilities.
	Data Imbalance	Financial Transaction Data	Disparities in representation of fraudulent vs. legitimate data make fraud detection more difficult.	Significant class imbalance and temporal dynamics mirror real-world complexities.
	Temporal Dynamics	Financial Transaction Data	Continuous evolution of fraud behaviors over time challenges adaptability of detection systems.	Changing patterns in the transaction data over time challenge the robustness of detection systems.
[10]	Zero-Day Exploits	Software and banking systems	Attacks that exploit software vulnerabilities unknown to the vendor, allowing cybercriminals to compromise systems before patches are developed.	Zero-day exploits take advantage of vulnerabilities in software before fixes are available
	Man-in-the-Middle Attacks	Communication channels	Cybercriminals intercept communication between a bank and A customer to steal information or manipulation of transactions	Man-in-the-middle attacks involve criminals inserting themselves between customers and banks
	DDoS (Distributed Denial of Service)	Banking servers and infrastructure	Cyber-attacks that flood banking servers with traffic to disrupt services, preventing access to critical financial functions like online and transactions.	DDoS attacks became the most frequent cyber incidents in 2020

	Phishing Attacks	Online banking systems	Fraudulent emails or websites designed to trick customers or employees into providing sensitive information such as login credentials or financial data.	Phishing Attacks where the most frequent type of incident

3.2 Findings of classification of vulnerabilities in banking system

References	Type of vulnerabilities	Place of vulnerabilities	description of vulnerabilities	Impact of vulnerabilities
[1]	Application Vulnerabilities	Web applications	Weak points like SQL Injection or Cross-Site Scripting XSS) that can be exploited to access data	Data breaches and disruption of critical services.
	Configuration Errors	System and network configurations	Misconfigurations, such as open ports or insecure default settings	Exposure of systems to breaches and data theft
	Access Control Weaknesses	Systems and databases	Weaknesses In Access management, such as excessive Der missions or weak password policies	Unauthorized access to sensitive data.
	Human Error	Employees and users	Mistakes caused by negligence or lack of awareness, such as; licking n malicious links or entering sensitive data on fake websites	Data leakage and creation of new vulnerabilities.
[2] [8]	Weakness in email authenticating	Email systems	Weak verification procedures allow intruders to send emails that appear legitimate within the system.	Theft of sensitive data and its potential leakage to external parties.
	Security updates weakness	Software and applications	Failure to regularly update systems, leaving exploitable vulnerabilities.	Exposing the system to breaches and theft of sensitive information.

	Weak user access management	Access control systems	Granting unnecessary privileges to users, increasing the likelihood of unauthorized access.	Internal system breaches and data manipulation
	Weak data encryption	Databases	Reliance on weak or outdated encryption protocols to protect stored data.	Decryption and theft of data become possible
[3]	Lack of SSL Encryption	Websites and Payment Systems	Absence of SSL certification, leaving sensitive data like payment details exposed during (transmission	Unauthorized access and potential breaches of sensitive financial data during online transactions.
	Poor Data Backup Practices	Servers and Storage Systems	Absence of a reliable backup system, making data recovery difficult in he event of an attack	Prolonged downtime and additional cos to recover data aft ransomware or both breaches.
	Vulnerable Mobile Applications	Mobile Banking Platforms	Applications with weak security measures that allow unauthorized accesso user data	Loss of personal and financial information, including theft of OTPs and unauthorized
[4][6]	Weak IoT Security	IoT devices in fintech systems	Vulnerabilities in IoT devices create entry points for unauthorized access.	Allows access to critical systems, compromising financial data.
	Insufficient Access Controls	Authentication mechanisms	Poorly designed access controls lead to unauthorized access to fintech platforms	Results in breaches that affect user trust and operational integrity
	Data Storage Weaknesses	Centralized databases	Weak security measures in database storage allow exploitation by cybercriminals. "	Enables large-scale data breaches and loss of customer data."

[5][8][1]	Weakness in System Design	Banking Systems and Infrastructure	Inherent flaws in the system architecture allowing attackers to exploit vulnerabilities for unauthorized access	Potential denial of service, unauthorized ace to sensitive data, c system failure
	Outdated Software	Servers and Applications	Lack of regular updates leaves systems exposed to exploitable bugs and vulnerabilities.	Higher susceptibility to cyberattacks an compromised data integrity.
	Weak Authentication Mechanisms	User Accounts	Use of inadequate password policies or lack of multi-factor authentication mechanisms.	Increased risk of unauthorized account access, leading to potential financial losses.
	Third-party System Dependencies	External Service Providers	Reliance on external platforms (e.g., PayPal) for transactions create japs outside direct control.	Increased risk of breaches and compromised security due to dependency on external systems
[7]	Outdated Software	Banking software systems	Use of outdated software that makes the system vulnerable to cyberattacks.	Facilitates exploitation of vulnerabilities by attackers, leading to data breaches or system compromise.
	Weak Authentication	Authentication mechanisms	Reliance on weak passwords or lack of multi-factor authentication.	Increases risk of identity theft and unauthorized access to accounts
	Weak Network Security	Network infrastructure	Absence of security measures like firewalls or intrusion detection systems.	Enables attacks such as DDoS disrupting services or stealing sensitive data.

[9]	Exploiting complex patterns	Traditional detection systems	Traditional systems fail to detect complex or emerging fraud patterns due to static criteria	Reduced efficiency in detecting new frauds, leading to financial losses and loss of trust
	Datasets	Datasets	Datasets contain biases, such as distribution imbalances and group disparities	Poor model performance on certain groups and weak generalization to new data
	Data imbalance	BAF dataset	Fraudulent transactions are significantly fewer than legitimate ones	Decreased model accuracy and increased risk of undetected fraud
	Dynamic temporal patterns	Transaction temporal data	Changing fraud behavior over time makes previously detected patterns ineffective	Reduced ability to detect new fraud patterns promptly
[10]	Zero-Day Exploits	Software in use	Exploiting software Vulnerabilities before vendors can patch them.	Data theft, undetected attacks
	Weak Physical Security	Data centers and physical infrastructure	Insufficient protection of digital assets and infrastructure.	Equipment destruction or theft, unauthorized access.

3.3 Findings of classification of countermeasures for banking system

References	**Type of countermeasures**	**Place of countermeasures**	**description of countermeasures**	**Impact of countermeasures**
[1]	Technical Controls	Systems and Networks	Includes encryption, firewalls, and intrusion detection systems	Protects sensitive data and prevents unauthorized access.
	Legal and Regulatory Measures	Legislation and Regulations	Compliance with regulations such as data protection laws and mandatory incident reporting	Reduces financial and legal risks, and increases customer trust.

	Organizational Measures	Organizational Structure of Financial Institutions	Includes security awareness training incident response planning, and risk management.	Enhances security culture and ensures business continuity in the face of threats.
	Advanced Technical Measures	Digital Infrastructure	Utilizes technologies such as artificial intelligence and anomaly detection to improve defenses.	Improves detection of advanced attacks and reduces vulnerabilities
[2]	Employee Training .	Financial Institutions	Regular cybersecurity training to educate staff on threats and Responses	Reduces human error and increases threat awareness
	Strict Security Policies	All Departments	Continuously updating policies to include strict access controls and encryption	Enhances protection against breachas
	Advanced Technologies .	IT Departments	Utilizing SIEM, IDS, and IPS systems for real-time threat detection	Improves threat detection and response
	Incident Response Plans	Upper Management	Developing and implementing disaster response plans and testing them regularly	Ensures operational continuity and reduces downtime
[3]	Regular Updates	Financial institutions' websites	Ensuring that all software and website details are updated regularly to close security gaps and prevent exploitation by attackers.	Minimizes the exploitation of security vulnerabilities by cybercriminals.
	Strong Passwords	Systems and applications	Using strong and complex passwords to reduce the likelihood of hacking attempts on Financial systems and applications	Enhances the institution's reputation and protects clients from cybercrimes

	SSL Certificates	Networks and websites	Implementing SSL certificates to secure networks, especially for financial transactions, ensuring encryption preventing unauthorized access	Enhances protection during data transmission and prevents data leaks to attackers
	Securing Customer Information	Data storage systems	Encrypting sensitive data and storing it only when necessary to prevent data leaks and unauthorized access	Prevents attackers from accessing customer data and reduces financial theft risks."
	Backup and Restore .	Databases and servers	Establishing regular backup systems to recover data in case of ransomware or phishing attacks without paying ransom	Reduces data loss impact and allows quick recovery without paying attackers.
	VPN for Data Transfer	Internet networks	VPNs to secure data transfer, making it difficult for attackers to trace or intercept Using user information	Reduces the risk of data theft during transmission and protects user identities.
[4]	Artificial Intelligence (Al) and Machine Learning (ML)	Threat detection and data security systems	Algorithms for analyzing patterns and adaptively detecting threats.	Enhances the ability to detect unknown attacks and reduces response time to incidents.
	Blockchain Technology	Financial transactions and smart contracts	Provides a decentralized, tamper-proof ledger supporting smart contracts for secure operations.	Reduces chances of tampering and fraud while ensuring data and transaction integrity.
	Biometric Authentication	User identity verification systems	Utilizes fingerprints, facial recognition, and voice recognition for	Improves security and offers a user-friendly experience, but

			secure user authentication.	raises privacy and data protection challenges
	Quantum-ResistantCryptography	Future encryption systems	Development of encryption algorithms resistant to quantum computing capabilities	Strengthens data security against potential quantum computing threats
	Behavioral Analytics	Anomaly detection systems	Analyzes user behavior patterns to proactively detect potential threats	Reduces the likelihood of unknown attacks through improved proactive monitoring.
	Decentralized Identity Management	Identity management systems	Employs blockchain-based solutions for decentralized and self-sovereign identity management.	Empowers users to control their personal data while reducing the risk of breaches.
[5]	Cyber Monitor	Deloitte CIC (Kenya)	A real-time security information and event management solution that detects, analyzes, alerts, reports, and initiates responses	Helps organizations develop a risk-based cybersecurity plan to prevent, detect and respond to attacks
	Cyber Watch	Deloitte CIC (Kenya)	A threat intelligence feed to identify potential attacks before they happen	Provides continuous vulnerability scanning and control
	Cyber Respond	Deloitte CIC (Kenya)	A tool for responding to cyber events and defending systems and networks	Minimizes financial impact from simultaneous attacks on systems and processes
	Biometric Security	Smart Online Banking System (SOBS)	Uses biometric fingerprints and digital signatures for every transaction	Reduces potential threats from intruders

	Firewalls and Routers	Network entry points	Configures firewalls and routers to control access and prevent threats	Reduces attacks on network entry points
	Least Privilege Policy	Device and system applications	Applies the principle of least privilege to ensure rights management	Identifies and minimizes unauthorized access
	Vulnerability Scanning	Application systems	Implements continuous vulnerability checks in applications and keeps them updated	Optimizes operational conditions and ensures system validation
[6]	Multi-layered security framework	Internal domain (LAN)	Implementation of a multi-layered framework to protect the system core from attacks	Enhances system security and reduces the likelihood of successful attacks
	Two-factor authentication	Internal and user domain (LAN/User)	Enables authentication using two distinct factors	Reduces the risk of unauthorized access
	Malware detection tools	Internal and user domain (LAN/User)	Advanced tools for detecting viruses and Trojan horses	Limits the spread of malware and improves security
	Awareness campaigns	User domain	Increases user awareness of social engineering attacks and how to avoid them	Reduces incidents of attacks that rely on human errors
	Route-based packet filtering	Network domain	Detects and filters rogue routers	Reduces attacks targeting incorrect routing paths
	Independent data storage infrastructure	Internal domain (LAN)	Uses a dedicated infrastructure to store data and prevent leakage	Improves data protection and reduces risks related to data breaches
	Digital authentication certificates	User domain	Utilizes digital certificates to enhance authentication security	Enhances security during data transmission

[7]	Multi-Factor Authentication . .	Authentication Process	Utilizes two or more verification layers to confirm user identity	Reduces the risk of unauthorized access to accounts
	Encryption	Data Transmission and Storage	Converts data into unreadable formats accessible only by authorized parties	Protects sensitive information during transmission and storage.
	Intrusion Detection Systems (IDS)	Network Security	Systems that monitor suspicious activities and generate alerts.	Identifies potential threats and prevents attacks proactively
	Regular Security Audits	Organizational Practices	Conducts periodic reviews of security systems and processes	Detects vulnerabilities and enhances overall security infrastructure.
[8]	Fraud Detection Techniques	Banks and financial institutions	Using anomaly detection and Machine Learning techniques to monitor transactions and prevent money laundering	contributes to reducing financial fraud risks
	Multi-Factor Authentication	Digital payment systems	Implementing multi-factor authentication techniques to secure customer data	Improves data security and prevents unauthorized access
	International Collaboration	Across nations and institutions	Sharing information on cyber threats and coordinating international efforts	Strengthens coordinated responses to cyberattacks

[9]	Stacking .	Fraud detection systems in banking	An ensemble model that combines predictions from multiple base models into a meta-model to improve Performance	Improved detection accuracy to 98%, enhanced balance between precision and recall, and reduced model errors
	Voting	Fraud detection systems in banking	Aggregates predictions from multiple models using hard voting or soft voting to determine the final Outcome.	Enhanced accuracy by leveraging the strengths of multiple models
	Gradient Boosting	Fraud detection systems in banking	Iteratively improves errors from previous models by training sequentially to learn from past mistakes.	High accuracy in handling imbalanced datasets and identifying complex fraudulent patterns.
	Deep Learning	Fraud detection systems in banking	Uses multi-layer neural networks to analyze data and detect intricate fraudulent patterns.	Improved real-time fraud detection and increased system adaptability to new fraud strategies
[10]	Training and Education	Financial institutions in Hungary	Mandatory security training to enhance awareness against phishing, smishing. and spear-phishing.	Improving Resistance to Phishing attacks involves education. staff must be familiar with recognition and escalation of a phishing attack
	Simplifying ICT Landscape	ICT infrastructure of financial sector	Segmentation of networks and limiting access points to reduce attack surfaces	Reducing possible entry points into the ICT infrastructure minimizes unauthorized access and ensures better protection of critical systems.

	Tools of Security and Defense	Financial institutions' ICT systems	Implementation of advanced tools like intrusion detection, DDoS protection, and honeypots.	State-of-the-art technology must be applied to support high levels of security, defense and resilience.
	Partnership and Information Sharing	Financial sector collaboration networks	Cooperation with ethical hackers, auditors, and information-sharing platforms for better security	Purple team Exercises analyze part of the financial institution's security lines and solutions, improving incident management.

3.4 Mapping between the threats, vulnerabilities and countermeasures

Type of threats	**Type of vulnerabilities**	**Type of countermeasures**
Ransomware	Weak Encryption	Implement advanced encryption methods, such as quantum-resistant cryptography, and Periodically update encryption protocols.
Insider Threats	Weak Access Management	Enforce least privilege policies, regularly review permissions, and conduct employee training
Zero-Day Exploit	Lack of Regular Software Updates	Ensure regular software updates and use Vulnerability Management Systems (VMS) to detect and patch vulnerabilities.
Phishing	Weak User Authentication	Deploy multi-factor Authentication (MFA) and Education of users on Recognizing phishing attacks.
Ransomware	Neglected Data Backup Practices	Establish routine backup systems and test data recovery to ensure operational continuity.
Distributed Denial of Service (DDoS)	Inadequate DDoS Protection	Utilize Intrusion Detection/ Prevention Systems (IDS/IPS) and Web Application Firewalls (WAF)
Phishing via Email	Weak Email Authentication	Implement email authentication protocols such as SPF, DKIM, and DMARC.
Malware on Mobile Devices	Insecure Mobile Applications	Enhance application security using encryption and conduct regular security assessments
Man-in-the-Middle (MITM)	Weak Network Security	Secure data transmission with strong encryption protocols like SSL and VPN.
SQL Injection	Design Flaws in Systems	Strengthening database security using prepared statements and parameterized queries

Social Engineering Attacks	Human Error	Conduct regular employee training and awareness campaigns to reduce mistakes caused by negligence or lack of awareness.
Data Breaches	Poor Data Backup Practices	Establish routine backup systems and test data recovery to ensure operational continuity.

6. Conclusion

This study examined the critical and emerging threats and vulnerabilities affecting the banking sector over the past three years, from 2021 to 2024. The primary objective of this article is to explore the major risks and vulnerabilities faced by banking institutions, analyze their potential impacts, and discuss key countermeasures and security controls employed within the sector. Additionally, the article interprets cybersecurity risk management strategies, including the processes of identifying, assessing, and mitigating potential risks. A systematic approach is adopted to evaluate and highlight vulnerabilities and threats specific to banking systems. By gaining a comprehensive understanding of these threats, vulnerabilities, and corresponding countermeasures, developers and security professionals can better anticipate cyberattacks, implement proactive defenses, and work toward effectively mitigating potential risks.

Funding

No funding.

Author contributions

Conceptualization, H.R.; methodology; R.S; formal analysis, H.R; investigation, R.S; resources, H.R; writing original draft preparation, H.R.; writing—review and editing, H.R and R.S. All authors have read and agreed to the published version of the manuscript.

Conflicts Of Interest

The authors declare no conflicts of interest.

References

[1] Kunz, J., & Heitz, M. (2021). Banks' risk culture and management control systems: A systematic literature review. *Journal of Management Control*, *32*(4), 439-493.

[2] Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A systematic literature review of e-banking frauds: current scenario and security techniques. *Linguistica Antverpiensia*, *2*(2), 3509-3517.

[3] Noory, S. N., Shahimi, S., & Ismail, A. G. (2021). A Systematic Literature Review on the Effects of Risk Management Practices on the Performance of Islamic Banking Institutions. *Asian Journal of Accounting & Governance*, *16*.

[4] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309.

[5] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. Authorea Preprints.

[6] Alkhdour, T., AlWadi, B. M., & Alrawad, M. Assessment of Cybersecurity Risks and threats on Banking and Financial Services.

[7] Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. *Information & Computer Security*, *25*(3), 240-258.

[8] Shrestha, S. (2019). Communication in banking sector: A systematic review. *Shrestha, S., Parajuli, S., & Paudel, U.(2019). Communication in Banking Sector: A Systematic Review. Quest Journal of Management and Social Sciences*, *1*(2), 272-284.

[9] Alhashmi, A. A., Alashjaee, A. M., Darem, A. A., Alanazi, A. F., & Effghi, R. (2023). An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures. Engineering, Technology & Applied Science Research, 13(6), 12433-12439.

[10] Somogyi, T., & Nagy, R. (2022). Cyber threats and security challenges in the Hungarian financial sector. Contemporary Military Challenges/Sodobni Vojaški Izzivi, 24(3), 15-29.

Biographies

Dr. Aitizaz Ali received the master's degree in computer systems engineering (with distinction) from GIK Institute, Topi, Khyber Pakhtunkhwa, Pakistan, and the Ph.D. degree in cybersecurity and blockchain technology from the School of IT, Monash University Malaysia, Jaya, Malaysia. He is a Lecturer with the School of IT, UNITAR International University, Petaling Jaya, Malaysia. He is the author of several Journal papers and international Conferences. He has authored or coauthored more than 20 research papers, including in highquality journals. His research interests include blockchain, cloud Ccomputing, cybersecurity, cryptography, deep learning, AI, and healthcare systems. moreover. He was the Reviewer of IEEE Internet of Things Journal, IEEE Transactions on Network Science and Engineering, IEEE Access, IET, and Human-centric Computing and Information Sciences Journals for several years. aitizaz.ali@apu.edu.my

Dr. Rami Shehab is working as a lecturer at the College of Computer Sciences and Information Technology, King Faisal University (KFU), Saudi Arabia. He has published several papers in well reputed journals and conferences. His research interests include cybersecurity, cybersecurity risk assessment and cryptographic. Rtshehab@kfu.edu.sa