MITIGATING CYBER THREATS AND ATTACKS IN SMART BANKING: BEST PRACTICES AND STRATEGIES

[1]OGUNNIYI, P.F and [2]OGUNNIYI, D, O.
1. Manchester Metropolitan University, Manchester, United Kingdom
2. Teesside University, Middlesbrough, United Kingdom

Abstract

Smart banking is an important critical national infrastructure that provides bank users with an easy and convenient experience. In this paper, the cyber threat and attacks associated with smart banking are explored. The paper also analyzed the risks associated with the threats and attacks identified with a focus on risk management strategies that can be implemented to mitigate them. The paper also covered the topic of security culture in relation to smart banking and how it might affect the efficiency of technical security measures. Important technical security controls like the use of encryption, firewall, and anti-malware are also discussed. Proper technical security controls including multifactor authentication, Behavioral biometrics are recommended.

Keywords: *Smart Banking, Man-in-the-middle attack, risk assessment, threat, vulnerability, firewall, tokenization, secure element.*

INTRODUCTION

The CNI (Critical National Infrastructure) banking sector has undergone a significant transformation recently as it transitioned from traditional banking to smart banking. In the past, customers had to physically visit bank locations to make transactions. This was a challenge as customers who lived in remote areas had to travel long distances to transact. The presence of long queues in the banking hall made it difficult for bank personnel to deliver efficient services and a good customer experience. Due to advancements in technology, the internet, and nations that are willing to implement cashless systems, smart banking has altered how clients interact with banks. With smart banking, clients can use their mobile devices, computers, or other wireless devices to access banking services whenever they want, from anywhere (Alzoubi *et al.*, 2022).

The rapid digitization of financial services has transformed traditional banking into what is now widely referred to as smart banking**,** where services are delivered electronically through mobile applications, online banking platforms, biometric authentication, automated teller systems, and cloud-supported infrastructures. Smart banking offers increased convenience, cost efficiency, and real-time service delivery; however, it also significantly expands the cybersecurity risk landscape (Sharma & Gupta, 2021).

As banks store and process sensitive financial information, they are prime targets for cybercriminals who exploit

system vulnerabilities, weak authentication mechanisms, social engineering tricks, and gaps in employee or customer security awareness (Ojeme & Ibidapo, 2022). Common cyber threats in smart banking now include phishing attacks, ransomware, identity theft, Distributed Denial of Service (DDoS) attacks, and fraudulent electronic fund transfers (Alhassan & Ahmed, 2023).

Although Smart banking offers a more convenient banking experience for both customers and bank staff, its dependence on the Internet makes it a big target for cybercriminals and other malicious actors. A successful breach in smart banking can lead to financial loss, non- financial loss (e.g. customer's data, transaction information etc.), and loss of customer trust in the organization (Ghelani *et al*., 2022). However, research indicates that technology alone cannot secure banking systems; effective cybersecurity also requires policy enforcement, employee training, regulatory compliance, and continual risk assessment (NIST, 2020; ISO/IEC 27001, 2022).

To safeguard against this risk, smart banking organizations must have in place good cybersecurity risk management practices, establish a strong security culture, and implement strong technical control. This paper aims to identify the latest cyber security threats and attacks to smart banking and to propose the latest information security controls to mitigate these threats.

COMPONENT OF SMART BANKING

Smart banking comprises different technologies and services that provide users convenience, speed, and security, like online banking, mobile banking, and contactless payments. In this paper, we'll focus mainly on the ones listed below.

1. *API*: Benmoussa (2019) defines an API, or application programming interface, as a "set of guidelines and standards allowing various software programs to connect". An API helps to simplify software development and facilitate the integration of various systems and services for developers. Thanks to APIs, users can access their accounts, send money, and complete other transactions using their mobile devices, making integrating banking services with mobile applications easier. Additionally, APIs make integrating banking services with other platforms, like e-commerce, betting, and other financial services easier (Kassab & Laplante, 2022; Behbehani *et al*., 2022).
2. *Smart Bank Payment* (Contactless): A big addition to smart banking is the introduction of contactless payment, which has simplified the payment process. Contactless payment is possible with the help of Near Field Communication (NFC) technology. According to Chabbi *et al*. (2022), NFC is a contactless communication technology included in the RFID (Radio Frequency Identification) technology. It is used for data communication between two NFC devices placed at a short distance". Payments are simple and quick with just a tap of a bank card or mobile device (Sportiello, 2019; Guers *et al*., 2022).

I. THREATS AND ATTACKS IN SMART BANKING AND FINANCE

The increasing reliance on smart banking on the internet makes it vulnerable to a range of cyberattacks. While some of these threats and attacks may not pose a significant risk to the technology, many others can cause severe damage. A system that guarantees the security and privacy of client data with 100% accuracy is required given the rise in network and internet-connected devices. Data security is one of the biggest issues facing the smart banking sector. Data sharing must be done safely, adhering to the three main security tenets of confidentiality, integrity, and availability. For instance, only authorized workers are allowed to access customer data, and any unlawful access can result in data breaches and identity theft. Moreover, data must not change from one point to another. For instance, severe consequences, such as inaccurate account balances, unauthorized transactions, and money loss, may result from tampering with a customer's financial data during transmission. Moreover, connected devices put the security of smart banking at risk. Smart watches and other Internet of Things (IoT) gadgets can put confidential financial information at risk of security breaches. These devices can send data that hackers can intercept and use to steal consumers' financial information. This section reviews the different types of threats and attacks to smart banking.

Classification of information security threats and attacks

a. Common Security Threats and Attacks
b. API security Threat and Attack
c. *Smart Bank Payment* (Contactless) Threat and Attack

a) **Common Security Threats and Attack**

1. **Smart banking malware:** Malware is malicious software an attacker uses to steal sensitive information by gaining unauthorized access to the system. Unauthorized access is achieved by exploiting a weakness or vulnerability, including unpatched software, misconfiguration, human error, and so on in the banking network. Successful malware attacks can be used by the attacker to steal information like login credentials, transaction data, card information, bank customer data etc. The attack affects the confidentiality part of the CIA triad (Alzoubi *et al.*, 2022; Malinka *et al*., 2022).
2. **Distributed Denial of Service*:*** The threat/attack focuses on the availability part of the CIA triad by preventing authorized bank users (customers and staff) from accessing authorized data. This attack overloads the smart banking networks with unnecessary traffic from multiple sources than they can handle, disrupting operations (Malinka *et al*., 2022; (10). This attack exploits the vulnerability of the bank server, network or website bandwidth capacity (2). A successful DDOS attack can lead to financial loss in the banking sector; it can also lead to reputation damage because customers may be hesitant to do business with a bank that has been targeted by a cyber-attack. According to a report by David Goldman on September 28, 2012, in business, Financial Institutions like Bank of America, JPMorgan Chase, Wells

Fargo, U.S. Bank and PNC Bank all suffered from DDOS attacks which makes their website unreachable for many customers. The attacker overwhelmed the bank's server by pointing thousands of high-powered application servers at it.

3. **Ransomware attack:** In this attack, the attacker used any of the other attack methods to gain unauthorized access to the banking network and encrypts all the information used by the banking organization and demands payment in exchange for the decryption key (Khan *et al*., 2020; Malinka *et al*., 2022). A successful ransomware attack can lead to the loss of sensitive data, system downtime, and financial loss. The attack affects all components of the CIA triad (Khan *et al*., 2020). According to Lifars, three community banks out of California and Florida were targeted by ransomware groups called Darkside and Ragnar Locker in May 2021. The attackers uploaded the proof of the attack and stolen customer data on the dark web and demanded ransom.
4. **Social Engineering**: Social engineering is a method employed by cybercriminals to take advantage of the human element of information technology systems. As smart banking and online financial transactions have grown in importance, social engineering has emerged as a major security risk for these systems. Social engineering is the practice of manipulating bank users into sharing private information, granting unauthorized access to systems, or taking other actions that could compromise system security. To gain their victims' trust and control, attackers may use a range of tactics, such as phishing emails, pre-texting, luring, or even impersonation. (Salahdine & Kaabouch, 2019). Phishing is a common social engineering attack that uses email, text messages or social media to trick bank customers into releasing sensitive information. The banking sector is one of the top organizations affected by phishing. According to Statista, the Banking sector is the third most affected organization affected by phishing attacks in 2022 with 10.29%. A successful phishing attack in smart banking can lead to financial loss to both the victim and the banking sector. For example, according to a report from Straits times, "A total of 790 people fell prey to phishing scams targeting OCBC Bank customers, with losses tallied at $13.7 million.". The attackers achieve this by sending SMS to all the victims by impersonating the bank. It was discovered that all the victims reveal their login credentials and one-time pin to the attacker which the attacker used to perform an account takeover.
5. ***Insider Threat*:** Smart *Banking* is among the CNI that handles a lot of sensitive information. Insider threats in smart banking arise when people with authorized access to confidential information, such as employees or contractors, intentionally or unintentionally misuse or disclose such information. Insider threats can result in financial or reputational harm to the bank and its customers. In addition to financial and reputational harm, insider threats can also result in legal and regulatory consequences, such as fines and lawsuits. Furthermore, insider threats can

also disrupt business operations, compromise sensitive data, and undermine the overall security posture of the bank.

b). **API Security Threats and Attacks in Smart Banking**

The OWASP (Open Web Application Security Project) conducted a statistical analysis of API threats and categorized them into different groups. The OWASP threats classification includes:

1. **Broken object level Authorization *(BOLA) and broken Authentication threat*:** The attacker aims to bypass the authentication mechanism the smart banking API uses by using methods like brute forcing, session hijacking or exploiting a weakness in the API endpoints. A successful authentication attack on smart banking has severe consequences like unauthorized access to sensitive customer data, financial information, and other sensitive data. In some cases, a successful authentication and authorization attack on customers' accounts can allow the attacker to perform unauthorized transactions like transferring money or stealing the customer's funds. According to a report by businesswire, an ethical hacker named Alissa Knight performed research on the security of bank API. Alissa managed to infiltrate 55 banks' APIs and perform unauthorized activities like changing customer PINs and transferring money in/out of the customer's account. Alissa penetrates the bank API by finding a BOLA vulnerability in the system. She managed to use the same vulnerability to penetrate 55 banks' API.
2. ***Injection attack*:** In this attack, the attacker sends malicious code or commands to the API request or response endpoint. Examples of injection attacks include SQL injection, NoSQL injection, OS command injection etc (Alam *et al*., 2022). A successful injection attack on smart banking can lead to unauthorized access to sensitive customer data, financial information, and other sensitive information such as bank details, transaction information, customer password etc.
3. **Excessive Data Exposure:** This API vulnerability may lead to serious threats. In data exposure, the API endpoint displays excessive data which the attacker can exploit. The attacker can use the excessive data to perform activities like changing customer data, transferring money etc.

c). **Smart Bank Payment (Contactless) Threats in Smart Banking**

1. **Replay attack:** In this attack, the attacker intercepted the communication between the contactless payment system and the terminal and used the information gathered to perform an unauthorized transaction (Chabbi *et al*. (2022). For example, if a customer purchases a product from a merchant using a contactless payment card and the attacker intercepts the transaction data during the communication between the card and the payment terminal, the attacker can later replay the data to initiate a new transaction without the customer's knowledge. In smart banking, the effect of a replay attack is significant because the attack is difficult to detect and mitigate. If the attack is persistent it can lead to reputational damage, legal and regulation consequences against the smart banking organization (Chabbi and Araar, 2022). The fig 1 below gives a

pictorial description of a replay attack.

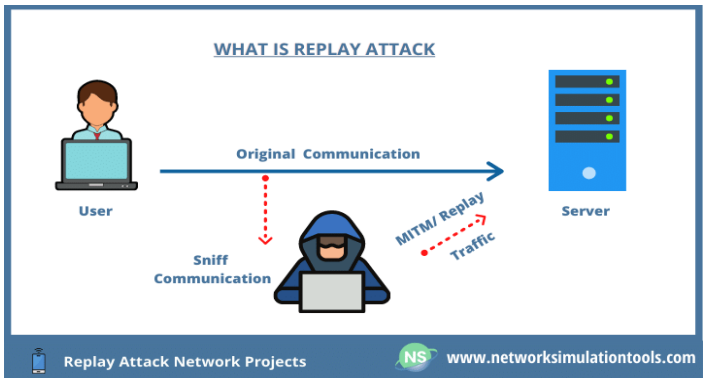

Fig 1: Example of Replay attack

2. **Physical Theft:** The biggest threat to contactless payment is the loss of the NFC device because of the lack of a verification system; it is easier for an attacker to perform illegal transactions with the stolen card.
3. **Relay attack:** A relay attack also known as the two-thief attack is a form of MITM attack where an attacker intercepts and relay communication between the payment card (NFC) and the payment terminal (Churaev *et al*., 2021). In this attack, the attacker records the cardholder information using a relay device and sends the information captured wirelessly to a third-party device (e.g. smartphone), that is placed near the payment terminal. The third-party device then used the information received to communicate with the payment terminal to make unauthorized transactions. The attack is targeted more at smart banking customers rather than the smart banking organization. A relay attack can cause a lot of reputation damage against the smart banking organization because the customer may not understand the attack and may hold the smart banking organization responsible ((Chabbi & Araar, 2022; Ahmed & Ibrahim, 2022). The fig below gives a pictorial description of a relay attack.

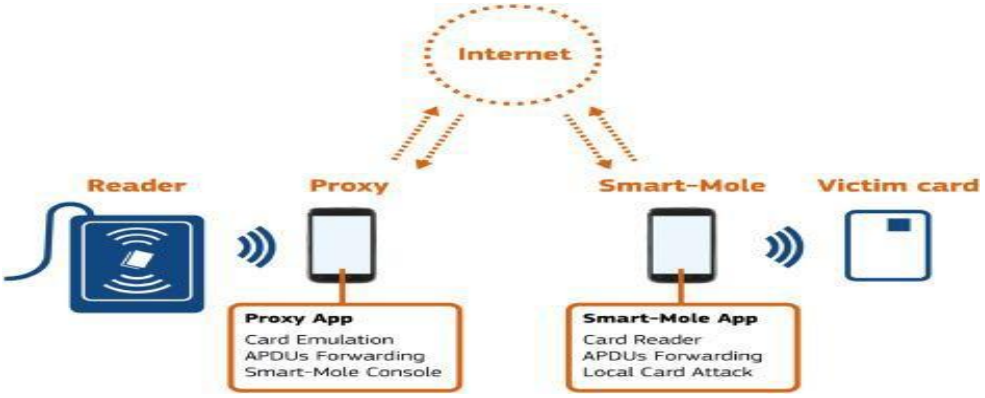

Fig 2: Example of Relay attack

Risk management can be defined as the process of identifying potential risks to smart banking, accessing the risk in terms of likelihood and impact on smart banking, and taking necessary action to minimize or reduce the risk (Legowo & Juhartoyo, 2022). The risk management process in this paper is performed following ISO 27001 and ISO 31000 frameworks. According to the frameworks, risk management can be performed by following this process. (Ponsard & Massonet, 2022)

A. Assets Identifications

Identifying assets is a crucial element in risk analysis as it is necessary to know what needs protection before implementing security measures. Smart banking consists of a lot of assets, but the report is limited to the assets listed and described in Table 1 (Georgiadou *et al*., 2020)

Table 1: Asset Identification

Asset	Description
Customer Data	To deliver individualized services and insights, smart banking primarily relies on client data. However, because this information is also very sensitive, it needs to be secured against theft or illegal access.
Transactions	Smart banking offers a variety of channels via which users can conduct transactions, including mobile apps, online banking, and ATMs. Maintaining customer trust and preventing fraud rely on the security of these transactions.
Mobile Devices	Customers can access their accounts and conduct transactions on the go because of mobile devices like smartphones and tablets, which are essential to smart banking. To stop data breaches and other security problems, these devices must be secured.
Networking Devices	By allowing connection between various systems and devices, networking devices, such as routers and switches, serve as the infrastructure of smart banking. Maintaining the integrity of the entire network depends on the security of these devices.
Cloud Infrastructure	To grow and manage their operations, many banks use cloud-based services to store and process client data. Yet, protecting customer privacy and preventing data breaches require securing cloud infrastructure.
Physical Infrastructure	Physical infrastructure, such as data centres and ATMs, is also necessary for smart banking. To prevent unwanted access and guarantee business continuity.
API endpoints	APIs are essential to smart banking since they allow various systems to connect. For the protection of customer data and to stop data breaches, API endpoint security must be ensured.

B. Threat and Vulnerability Identification

Identifying potential threats and vulnerabilities to the system is a very important aspect of the risk management plan, understanding the sources from which threats to information system assets will come from is a key factor in determining how best to mitigate them. Vulnerabilities refer to flaws or weaknesses in a system that can be exploited by unauthorized individuals for their gain. Table 2 identified different types of vulnerabilities in

smart banking and their definition.

Table 2: Vulnerabilities Identification

Vulnerabilities	Definition
Human Error	Mistakes made by individuals, which can compromise the security of a system
Software Vulnerability	Weaknesses or flaws in software code that can be exploited by attackers
Network Congestion	Overload or saturation of network resources, which can lead to system disruption
Weak Access Control	Failure to implement proper access controls, allowing unauthorized access to data
Weakness in Authentication	Inadequate verification of user identity, allowing unauthorized access to a system
Weakness in Authorization	Inadequate controls over user permissions, allowing unauthorized actions

C. Risk Matrix

The following formula was used to calculate the level of risk.

Risk level = Risk Likelihood * Risk Impact

I. Likelihood Rating

Likelihood refers to the probability that a specific risk will occur. The probability is determined based on historical data, expert judgment, or other relevant information. Table 3 provides an analysis of the likelihood rating model and explains its various components.

Table 3: Likelihood Rating by Ogunniyi (2023)

Likelihood	Definition
Almost Certain(1.0)	The threat is expected in most circumstances.
Likely(0.7)	The threat can occur in most circumstances.
Possible(0.5)	There is a probability that the threat will occur at some time.
Unlikely(0.3)	There is a probability that the threat could occur at some time.
Rare(0.1)	The threat only occurs in surprising circumstances

II. Impact Rating

Impact in risk assessment can be defined as the consequence of a risk. The impact is a very important

part of risk assessment. Because understanding the severity of risk can help determine how much attention and resources to place on the risk. Table 4 provides an analysis of the impact rating model based on a qualitative basis and explains its various components.

Table 4: Impact Rating by Ogunniyi (2023)

Impact	Definition
High (100)	The impact could lead to a severe loss to smart banking in terms of CIA trad, financial loss, and Reputational damage.
Medium (50)	The impact could lead to minimum loss to smart banking in terms of CIA trad, financial loss, and Reputational damage.
Low (10)	The impact on smart banking organizations is low in terms of CIA trad, financial loss, and Reputation damage.

III. RISK LEVEL

Table 5: Risk Level

Likelihood	IMPACT			
	Low (10)	Medium (50)	High (100)	Risk Level
Almost Certain (1.0)	10 Low	50 Medium	100 High	High
Likely (0.7)	7 Low	35 Medium	70 High	High
Possible (0.5)	5 Low	25 Medium	50 Medium	Medium
Unlikely (0.3)	3 Low	15 Medium	30 Medium	Medium
Rare (0.1)	1 Low	5 Low	10 Low	Low

Interpretation of Risk Levels

i. **High-Risk Zone (Scores 51–100):** Events that fall into this zone—such as *phishing attacks*, *ransomware infections*, or *data breaches* require immediate attention and strong mitigation measures. For instance, a data breach rated as *Likely (0.7)* with a *High Impact (100)* produces a risk score of 70, which is classified as *High*. Such risks demand proactive security investments, continuous monitoring, and employee training to minimize exposure.

ii. **Medium-Risk Zone (Scores 11–50):** This category represents risks that occur less frequently or have moderate consequences, such as *unauthorized access attempts* or *malware infections* contained by internal defenses. These risks should be regularly monitored **and** controlled through preventive measures like firewalls, encryption, and regular software updates.

iii. **Low-Risk Zone (Scores 1–10):** Risks in this category—such as *minor technical glitches* or *unsuccessful hacking attempts*—have low probability and minimal impact. While they do not require immediate mitigation, banks should maintain baseline controls and periodic reviews to ensure these risks remain at a manageable level.

D. RISK ASSESSMENT

Table 6 shows the overall risk assessment using the risk matrix in Table 5. The table calculates the level of each risk to a smart banking organization.

Risk Rating Criteria

Risk scale =High(>50 to100),
Medium(>10 to 50),
low (1 to10)

Table 6: Risk Assessment Table

Threat	Asset	Vulnerability	Likelihood	Impact	Risk Level	Risk Mitigation
Phishing attacks	Customer Data	Human error	Almost Certain	High	High	• Educating all employees on how to identify and avoid phishing attacks. • Implementing strong Multi-Factor Authentication.
Malware attacks	Applications	Software vulnerabilities	Possible	High	High	• Performing Regular updates and patches. • Testing all updates and patches before usage • Installing adequate anti-virus and anti-malware.
Insider threats	Transactions Customer Data	Employee access and authorization	Possible	High	High	• Implement a least privilege access control model. • Monitoring the network packet for suspicious activities.
Denial-of-service attacks	Networks	Network congestion and resource depletion	Unlikely	High	Medium	• Implementing strong DOS security like packet filtering, rate limiting and load balancing. • Monitoring the network for irregular activities.
Data breaches	Cloud Infrastructure	Weak access controls and encryption	Likely	High	High	• Implementing strong access control and encryption for data at rest. • Implementing strong multi-factor authentication for access to data at rest.

Physical theft	Physical Infrastructure, Payment card	Access control weaknesses, Unauthorized access to contactless devices	Rare	High	Low	• Implementing strong physical security measures such as alarms, CCTV, access control etc.
ATM skimming	Physical Infrastructure	Tampering with hardware	Rare	High	Low	• Implementing strong physical security measures such as alarms, CCTV, access control etc.
Ransomware attacks	Applications, Network, Server	Exploiting software vulnerabilities	Possible	High	High	• Use strong network segmentation to prevent the spread of ransomware. • Performing Regular updates and patches. • Testing all updates and patches before usage • Installing adequate anti-virus and anti-malware.
Credential stuffing	Transactions	Weaknesses in authentication systems	Possible	Medium	Medium	• Monitoring logins attempt for suspicious behaviour
Unauthorized access	API Contactless	Weaknesses in authentication and authorization	Likely	High	High	• Implementing strong authentication measures. • Regular review and update access control
Data leaks or data breaches through APIs	API	Weaknesses in encryption, access controls, or vulnerabilities in third-party APIs	Possible	High	High	• Encrypting all sensitive data. • Sharing API endpoints with only trusted third parties.
Injection attacks through APIs	API	Weaknesses in input validation	Likely	High	High	• Implementing top-of-the-art input validation. • Conduct regular penetration testing.
Replay attacks	Payment card	Weaknesses in transaction validation	Unlikely	High	Medium	• Monitoring contactless activities for suspicious behavior. • Implementing strict transaction validation protocol.

E. Handling periodic changes:

As days go by, Threats and attacks on information communication system increase, and attackers find new ways to attack the system. The following can be used to handle periodic changes to the risk management plan:

a. ***Risk management regular reviews and updates:*** It is very important to review and update RM frequently to make sure it is up-to-date and relevant against new threats/attacks and vulnerabilities. This can be done by regularly researching new risks and updating the RM with the result.

b. ***Implementing new security measures*****:** new security measures should be implemented to mitigate the new threats and attacks identified.

c. ***Training and education*****:** Constant Training for the employees on new threats and attacks, and how to identify and mitigate them. This can include security awareness training, phishing simulations, and regular reminders about safe online behavior.

F. Incident Response*:*

The following process can be used to perform incident response in smart banking by the ISO27001 Framework:

1. **Identification:** This is an important aspect of Incident response. In incident response identification, a variety of ways is put in place for identifying incidents. Along with the automated incident identification by using tools like intrusion detection systems, it is important to note that incident identification is everyone's responsibility (both the technical and non- technical staff of the organization, Customer), it is important to set up an incident response team where all the incidents identified are reported.
2. **Assessment:** In this stage, all the members of the incident response team analyze the incident identified by determining its severity and impact on the organization.
3. **Response:** In this stage, the necessary response is taken by the severity, impact, and type of incident. E.g., Server restarts in case of a DDOS incident, card deactivation in case of card theft, checking CCTV in case of ATM skimming. The response may include containment of the incident, investigation to determine the cause, and remediation to prevent the incident from recurring.
4. **Reporting:** In this stage, all the incidents identified are recorded and reported to the relevant department and people. E.g. in case of an unauthorized login incident, a message can be sent to the affected person to change the password.
5. **Review and improvement:** The incident response plan should be reviewed and updated regularly to ensure that it remains effective and aligned with the organization's goals and objectives. Smart Banking will also conduct regular tests and drills to ensure that its incident response plan is effective and that its staff are trained to respond to security incidents.

All smart banking organizations must have an incident response plan (Staves *et al.*, 2022) which includes:

1. The list of the incident response teams.
2. **Roles and responsibilities***:* The plan should clearly define individuals' roles and responsibilities, including who is responsible for identifying and reporting security incidents, who will lead the response effort, and who will communicate with stakeholders.
3. **Severity and impact assessment**: Smart Banking will establish criteria for determining the severity and impact of security incidents. This will include factors such as the type of data involved, the number of customers affected, and the potential financial impact.
4. **Incident response procedures**: The plan should establish procedures for responding to security incidents, including containment, investigation, and remediation. This will include specific steps to be taken in response to different types of security incidents.
5. **Communication procedures:** The plan will contain a process for communicating with relevant departments, including customers, regulatory authorities, law enforcement agencies and members of the incident response team (in case of incident identification). This will include templates for notification messages and protocols for communicating with this department in a timely and effective manner.

IV.SECURITY CULTURE IN SMART BANKING

The ideals, attitudes, and behaviours exhibited by individuals inside an organization regarding security are referred to as security culture. A willingness to abide by security policies and procedures and a shared commitment to safeguarding sensitive data and assets are features of a strong security culture. In smart banking, adopting strong security is important because of the level of sensitive data being handled. A strong security culture can help to mitigate risk in smart banking by adopting a culture of vigilance and accountability. In this section, different security best practices, policies and control are discussed (Walter, & Narring, 2020).

A. Risk-Based Approach

A very important security culture approach in smart banking is the Risk-based approach. The risk-based approach places a strong emphasis on determining and categorizing the most important cybersecurity threats and then applying controls to reduce those risks. To help ensure that controls are effective and relevant in the face of constantly changing cyber risks, this strategy involves regular evaluation and reassessment.

Reasons for risk-based approach:

1. **Prioritizing Resources:** The approach helps banking to prioritize their resources and concentrate on the most important component of their security program. This helps in banking because of the amount of available potential threats and limited resources to deal with them. Smart banking organizations can allocate resources more effectively and efficiently by determining the biggest risks.
2. **Decision Making:** Risk-based approach helps organizations to increase their decision-making through the impact of threat and vulnerability, enabling them to choose which risks accepting,

mitigates, or transfers.

3. **Evidence Based:** Through Risk-based approaches security decisions are made based on data and evidence rather than speculation or assumptions. This is crucial in smart banking because a security breach might have serious repercussions. Evidence-based risk management assists businesses in reducing uncertainty and improving decision-making.

B. Policies in Smart Banking

Policies are written documents that outline how an organization should handle and safeguard sensitive data and technology. Smart banking policies are designed to protect the security and integrity of financial transactions and sensitive information in compliance with applicable laws, regulations, and industry standards. Below are some of the important policies in smart banking.

i. Information Classification Policy

To avoid threats like unauthorized access and for easy implementation of the access control policy, it is important to categorize data used in smart banking based on their level of sensitivity. The policy should define the following:

1. **Classification Criteria:** Data classification based on their level of sensitivity must be strictly defined in the information classification policy. For Example, Mechanisms like confidential, public, Internal etc can be used to classify data and information based on their level of sensitivity.
2. **Information Security Procedure**: The information classification policy must specify the level of security that must be used to safeguard data and information based on their level of sensitivity. For example, confidential information must be protected with extra security measures like encryption while public information may not need restrictions,
3. **Employee Responsibility:** The information classification policy must clearly outline the roles of every employee in the company in managing sensitive data and information. This must include the type of data each employee can access, and how to access and transfer the information.
4. **Monitoring and Review:** The policy should incorporate monitoring and review procedures to ensure compliance with all information classification policies. Additionally, it should outline the consequences of non-compliance.

ii. Training and Awareness policy

This is one of the most important policies in smart banking, it is important to indicate that security is everybody's work, both the employee and the customer. General Data Protection Regulation (GDPR) requires all organizations to ensure that all personnel who access sensitive data are trained on how to handle that data securely. The organization should ensure that its staff and customers are informed about emerging threats and the methods used by attackers.

iii. Password Policy

Password authentication is one of the most critical components of information security. The use of passwords helps protect against unauthorized access to sensitive information. Customers in smart banking used passwords to protect their financial and personal information. The password policy contains a set of rules and guidelines on how passwords should be created, managed, and used by the member of the banking organization and the customers. The following are elements that should be considered in the password policy.

a. **Password strength and complexity:** it is important to note that the password policy stipulates passwords to be strong, complicated, and not guessable (Davis *et al*., 2022). A good password should include a letter (upper and lowercase), digits (1-9) and special characters.

b. **Password reuse:** it should be stated in the password policy that all users are prohibited from reusing old passwords to ensure that compromised passwords are not reused and that attackers do not have easy access to data.

c. **Password storage:** The policy should require that all passwords should be safely stored, such as through state-of-the-art encryption methods or hashing. It is important to use passwords that can easily be remembered to avoid writing them down.

d. **Password sharing**: It is essential to state in the password policy that sharing passwords with others is forbidden as this could result in unauthorized access and security breaches.

The following are some of the guidance for password management systems according to ISO 27001 Annex A 5.17

1. Users should have the ability to create and modify their passwords.
2. User must change their default password upon first accessing a system.
3. It's essential to change passwords when appropriate. For instance, after a security incident.
4. It is bad to reuse the previous password.
5. Passwords must be transmitted and stored through secure channels in a secure format.

iv. Access Control Policy

To avoid threats like unauthorized access and insider threat, it is important to have a policy that ensures that data are accessed by only authorized users. Access control policies are a set of guidelines that indicate how access to data, systems and applications should be managed in smart banking.

An access control policy typically comprises the following components:

1. **Access control models:** The policy should define the access control models that will be used to manage access, such as discretionary access control (DAC), mandatory access control (MAC), or role-based access control (RBAC).
2. **Authentication mechanisms:** The policy should specify the authentication mechanisms that will be used to verify the identity of users before granting access. This could include username and password

combinations, biometric authentication, or multifactor authentication.

3. **Authorization rules:** The policy should define the authorization rules that will be used to grant or deny access to specific resources based on the user's role or level of authorization.
4. **Access management procedures:** The policy should outline the procedures that will be used to manage access, such as the creation and deletion of user accounts, password management, and access revocation.
5. **Audit and Monitoring:** To ensure policy compliance, the policy must specify the audit and monitoring mechanisms that will be used to track and report access occurrences.

v. Third-party policy:

One of the important characteristics of smart banking is the ability to incorporate its technology with third-party technology. To reduce threats from third-party organizations, it is important to have a policy that outlines the procedures and guidelines for managing their relationship. The policy should define the following.

1. *Vendor Selection*: The Third-party policy must clearly outline different criteria for selecting a third-party vendor. The criteria must be based on the vendor's capabilities, reputation and compliance with industry regulations and standards.
2. *Vendor Requirement:* The policy must clearly state all the requirements the third-party vendor must adhere to. The policy must state requirements for data protection, security measures and reporting of any security incidents.
3. *Incident Response:* The policy must outline the necessary procedure to follow in case of a third-party incident.

vi. *Acceptable Use Policy (AUP):*

AUP is an important policy that outlines the guidelines and procedures for the appropriate use of information technology (IT) resources in the organization. The policy should define the following.

1. Access and Authorization: The policy should clearly state who has access to IT resources and the step for granting and reversing rights.
2. Prohibited Activities: The policy should specify which activities are accepted and prohibited when using IT resources. Installing software and downloading files from unconfirmed sources should be strictly prohibited when using IT resources.
3. Email and Internet use:

Table 7 relates each policy discuss above with appropriate industry standards.

Policy	Related Standard	Description
Password Policy	ISO 27001	The standard outlines the important requirement for an information security management system, including the need for password policies to be implemented and enforced.
Access Control Policy	PCI DSS	The Payment Card Industry Data Security Standard outlines requirements for protecting cardholder data, including the need for strong access controls to limit access to sensitive information.
Information classification policy	GDPR	The General Data Protection Regulation requires organizations to classify personal data according to its level of sensitivity and implement appropriate safeguards to protect it.
Third-party policy	ISO 27001	This standard includes requirements for managing the risks associated with third- party service providers, including the need for contracts and agreements that address information security requirements.
Training and Awareness	PCI DSS	The Payment Card Industry Data Security Standard includes requirements for ongoing training and awareness programs to ensure that staff members understand their responsibilities for protecting sensitive information.
Acceptable use Policy(AUC)	IS0 27002:2022 5.10	This standard outlines guidelines for the acceptable use of information technology resources, including policies for protecting against malware, accessing sensitive information, and using personal devices on organizational networks

C. Managing Policy

In smart banking, the policy can be implemented and managed following these processes:

1. *Communicate the policies*: All the policies identified must be extensively communicated to all relevant personnel, including Employees, customers, and third- party vendors. The policies can be communicated through training sessions, presentations, and communications channels like email, phone calls and so on.
2. *Compliance Monitoring*: This is an important aspect of policy management; all departments must be monitored to ensure that they are being compliant with the policies. This can be done through regular audits and monitoring tools.
3. *Enforcing policy*: It involves the implementation of measures to ensure that employees, third-party vendors, and customers follow established policies and procedures. For example, a Bank customer's login can be configured to follow password policy by putting a constraint on the password field (e.g. password must contain at least one uppercase and one character, and the password must be 7 or

more characters).

4. *Implement necessary technical controls*: Appropriate technical controls like encryption, intrusion detection system, and use of a firewall must be implemented.

V. TECHNICAL SECURITY CONTROLS FOR SMART BANKING

Technical controls are technology security measures organization uses to protect their assets. Smart banking organization needs to have very strong technical security control because of the nature of the asset being protected. With strong technical security control, smart banking can provide a secure banking experience for their customer.

a. General technical security controls for smart banking

1. Firewall and intrusion detection system

A firewall is a security control method that monitors and controls network traffics coming and going out of the system based on some set of security policies (Nabi *et al*., 2022). The use of a firewall can help to prevent cyber-attacks like smart banking malware, Distributed denial of service and so on. In smart banking, the firewall can be used to secure unauthorized access to the network infrastructure that supports banking operations.

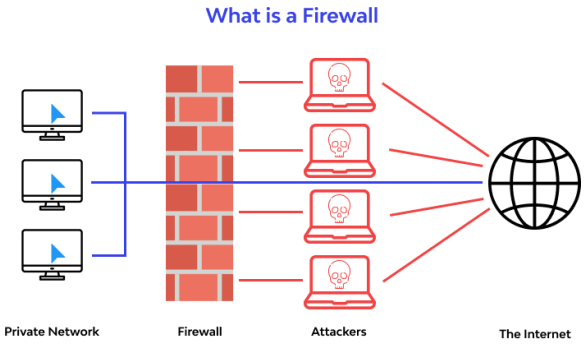

Fig 3: Firewall pictorial representation

a. **Advantages of firewall in smart banking**

i. Firewalls are used to protect sensitive banking assets (customer data, transactions etc) from unauthorized access.

ii. Firewall can be configured to monitor access to smart banking infrastructures like online banking, mobile banking etc, to restrict certain types of transaction or block traffics based on suspected Ip address.

iii. Firewall can also be important to smart banking in complying with regulatory requirements by providing network segmentation, access control and logging network activities for auditing.

b. **Disadvantages of firewall in smart banking**

i. **False positive and false negative:** Firewalls sometimes produce false positives by blocking legitimate traffic from accessing the network or false negatives which allow unauthorized networks from accessing the network. This situation is rare but possible.

ii. **Incomplete protection**: Firewall is limited to some cyber-attacks like malware detection, network scanning, and DOS but is not effective in some attacks like social engineering and insider threat.

iii. **Performance impact:** Firewall in some situations can impact network performance which is a very big problem in smart banking because of the number of users.

An intrusion detection system (IDS) is a security control for monitoring and identifying networks for malicious activities. IDS can be used in smart banking or detect attacks like malware, Denial of service etc. IDS monitor all system activities and reports any suspicious activities to smart banking security personnel.

The paper (Soewito & Andhika, 2019) introduced the use of a next-generation firewall (NGFW) by comparing it with the traditional firewall. The authors compare this firewall by performing a life experiment against attacks like DDOS, SQL injection and phishing. It was discovered that the next- generation firewall provides more security control than the traditional firewall in all measures. The NGFW overcome the weakness of traditional firewall by providing the ability to control based on application, not a port. It also performs deep packet inspection. It can also be integrated with the active directory server. NGWF also could perform the IDS role.

2. **Encryption and Secure socket layer (SSL) security:** Encryption is a security measure that uses mathematical computation to convert human-readable information into meaningless information to protect it from unauthorized access. Encryption is a very important security measure for smart banking because of the amount of sensitive data and information being used by the infrastructure. In smart banking, encryption can be used to protect both data in transit like credit card information and account login credentials that are sent over the internet and data at rest which are stored in the server. Encryption can help prevent attacks like MITM, insider threats and ransomware. There has been different encryption algorithm throughout the year which includes Caesar cypher, one-time pad, Data encryption standard, Rivest Shamir Adleman (RSA), Elliptic curve cryptography (ECC), and Advance encryption standard (AES). Selecting the best encryption algorithm for smart banking depends on some variables like the level of security, the speed of the algorithm and the feasibility of implementation. According to (Mouha, 2021), "AES is an encryption algorithm approved by the National Institute of Standards and Technology (NIST)".

A secure socket layer (SSL) is a protocol that is used to create a secure connection between the web server and web clients. Transport layer security (TLS) is an advancement of SSL. The protocol is used to protect smart banking information from attacks like eavesdropping and MITM. The protocol uses different combinations of encryption algorithms to protect data.

3. **Anti-malware**

This is an important security measure used in smart banking to protect against malicious attacks like malware, trojan horse, spyware, and virus. Anti-malware programs are designed to detect, prevent, and

remove malicious activity from the organization's system.

a. **Benefit of Anti-malware in smart banking**

i. **Real-life scanning and monitoring:** Anti-malware programs provide real-world monitoring of the smart banking system, identifying any suspicious activity and preventing malware from infiltrating the system.

ii. **Automated updates:** robust and advanced anti- virus system can receive regular updates to ensure it can detect the latest malware threats.

b. **Drawbacks of anti-malware in smart banking**

i. **Outdated Protection:** Anti-malware must always be updated with the latest malware definitions to protect against new and emerging threats. Attackers can use the vulnerability of outdated malware to manipulate the banking system and introduce new types of malwares to the system.

ii. ***Limited Protection:*** Anti-malware is limited to some specific attacks and cannot be used to protect against other attacks like social engineering, insider threat etc.

B. API technical security Control for smart banking

1. Authentication

The use of a strong authentication mechanism is important in improving the security of APIs in smart banking. API has a lot of security measures that can be used to protect the data and information of smart banking, these methods include the use of API keys, OAuth2 and JSON web tokens (JWTS).

C. Contactless payment technical security control for smart banking

1. Tokenization

Tokenization is a security measure used in contactless technology systems to protect sensitive data from unauthorized access. It happens when the bank customer makes a contactless payment using their credit or debit card. The card data is first encrypted with a secure encryption algorithm which is then replaced with a randomly generated token referred to as a payment token. The generated payment token is then used to represent the card data during the payment gateway. The token provider is responsible for generating, assigning, and managing the token (Akinyokun & Teague, 2017).

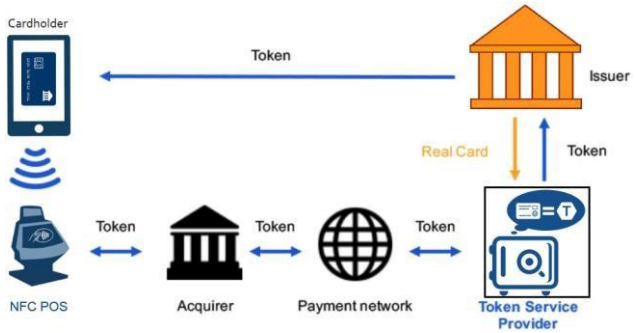

Fig 4: Tokenization representation by (Akinyokun & Teague, 2017)

a. Benefit of tokenization in smart banking

i. *Protection against fraud*: Tokenization helps smart banking to protect against contactless payment fraud in case of a data breach. It happens by replacing the payment data with a randomized token number which makes it hard for unauthorized personnel access to the payment data to use the data.

ii. **Compliance:** Tokenization provides a good security measure for contactless payment which help them comply with industry standards like PCI DSS which require all organization to use strong encryption and tokenization.

iii. **Reduced Liability:** Tokenization can help reduce the liability for merchants and payment processors in the event of a data breach. Replacing sensitive cardholder data with tokens reduces the risk of compromised payment data, reducing the potential for costly fines and legal fees.

a. Drawbacks of tokenization in smart banking

i. **Dependency:** if the security of the tokenization provider is compromised, it can put payment data at risk because tokenization is dependent on the security of its provider.

ii. **Limited scope:** The use of tokenization only protects a limited number of threats.

2. **Secure Elements**

A secure element is a hardware component used for storing and processing sensitive data (Alam *et al.,* 2022). The secure element is used in contactless payment to store sensitive information like payment information, credit, or debit card details and to perform secure transactions. When a payment transaction is initiated by a smart banking customer, the payment information is securely transmitted from the secure element to the payment terminal (Akinyokun & Teague, 2017)

a. Benefits of the secure element in smart banking

I. **Enhanced security:** The secure element is used to protect against attacks like skimming, cloning etc. Secure elements are built to be tamper resistance and be used. Configure to enforce strict security policies like encryption and authentication.

II. **Versatility:** The technology can be included in contactless payment devices like smartphones, smart cards, etc.

b. Drawbacks of the secure element in smart banking

i. **Limited storage:** The technology has limited storage space which can limit the functionality of contactless payment.

ii. **Cost:** The technology can be expensive for a business running on a tight budget.

D. Gaps in current security controls

Although all the security controls identified above are ways to increase the security of smart banking. Different gaps in these security controls can expose the smart banking information asset to threats and attacks. These include:

1. ***Lack of user awareness*:** Even with all the above technical security measures, smart banking still

relies heavily on customer interaction such as entering usernames and passwords for authentication, approving transactions etc. Many cyber attackers used the user's lack of security awareness to manipulate them to share sensitive information.

2. ***Patch management*:** most of the current technical security control requires constant patches and updates. If the updates are not done consistently, it may leave them vulnerable to attacks that exploit known vulnerabilities. Attackers can manipulate this vulnerability to access smart banking-sensitive information assets.

3. **Poor configuration management:** The current technical security controls are complex systems requiring high-level configurations and policies. Misconfiguration in these systems creates new vulnerabilities for attackers to exploit.

RELATED STUDIES

A study by Alhassan & Ahmed (2023) found that social engineering remains one of the most effective methods attackers use to breach banking systems, largely due to low user awareness and trust exploitation. Their research showed that customer-focused education and stronger identity verification controls significantly reduce fraud incidents.

Parsons *et al*. (2019) found that susceptibility to phishing is influenced by user awareness, security culture, and perceived threat severity. Their study highlights that technical defenses alone are insufficient; banks must strengthen security training and behavioural interventions to mitigate social engineering risks in smart banking systems.

Karia & Patel (2022) analyzed the adoption of multi-factor authentication in mobile banking platforms. Their findings revealed that while MFA reduces the likelihood of unauthorized access, its effectiveness depends on the method used—biometric and token-based authentication provide stronger protection compared to SMS-based OTPs, which can be intercepted.

A recent study by Bhasin & Goyal (2024) demonstrated that machine learning algorithms significantly improve fraud detection accuracy in online banking systems. However, they caution that models need continuous retraining because cyber attackers adapt to detection patterns.

Carcillo *et al*. (2021) demonstrated that hybrid machine learning models combining supervised and semi-supervised learning significantly improve fraud detection accuracy in financial transactions. However, the study warns that AI systems require regular retraining to remain effective against evolving cyber threats.

Research by Nwankwo & Okorie (2021) emphasizes that even strong cybersecurity tools fail without organizational governance. Their study found that banks with dedicated cybersecurity teams, clear policies, and employee cybersecurity awareness programs had significantly fewer security incidents.

The UK's Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) in 2021 issued policies requiring banks to develop robust operational resilience and incident response frameworks**.** These regulatory guidelines highlight governance as a core component of cyber threat mitigation in smart banking.

Ifinedo (2012) examined the determinants of security policy compliance in organizations and found that management support, clear policy communication, and organizational culture strongly influence compliance behaviour, which is essential for cyber resilience in smart banking.

Bouveret (2018) developed a framework for estimating the financial impact of cyber incidents in banking. The study concludes that banks face disproportionately high losses due to the sensitive nature of financial data and interconnected digital infrastructures. The research emphasizes the need for continuous risk assessment and resilience planning in smart banking environments.

Mavroeidis & Bromander (2017) proposed a cyber threat intelligence framework that helps organizations anticipate emerging attacks. Their findings support threat monitoring and intelligence-sharing networks as critical strategies in modern banking security operations.

A recent ENISA (2023) report identifies ransomware, supply chain attacks, and credential theft as the most prevalent cyber threats affecting European and UK financial institutions. The report emphasizes continuous monitoring and cross-institutional intelligence sharing.

CONCLUSION

In this paper, a sector of critical national infrastructure called smart banking was reviewed. Some of the threats and attacks against smart banking were discussed and some real-life cases were reviewed. Different security measures for preventing and mitigating the threats and attacks identified were discussed. The security measures discussed include a risk management plan, incident response plan, security culture best practices and important technical security controls identified. However, it should be noted that the constantly changing nature of cybersecurity threats requires regular evaluation and improvement of security protocols. As a result, organizations in the smart banking sector must always be on the lookout for new forms of fraud and adapt to combat them. Smart banking organizations may better secure their essential assets and keep their customers' trust by adopting the suggested state-of-the-art technological security controls and building a strong security culture.

RECOMMENDATION

1. Multi-factor authentication (MFA)

The use of a password mechanism for authentication in smart banking does not provide enough security for the infrastructure. Attackers can use various ways to get the login details. There is a need for an extra layer of security to protect this single form of authentication. Multi-factor authentication is a technical security control mechanism used in smart banking to provide an extra layer of security (Rajabboyeva, 2023). In this control, a multiple authentication method is used to confirm the identity of a user before giving them access to their authorized account. Multi-factor security control uses two or more of the following authentication method:

a. Password or Pin

b. Physical token

c. Biometric data E.g. fingerprint or facial recognition.

d. One-time pin

In real-life cases, the method is most effective when performing online transactions. MFA in online banking requires users to provide a one-time code sent to their mobile device via SMS, Mail, or mobile app in addition to their payment card pin (Jana, 2021).

2. Behavioural Biometric

It is a type of biometric authentication that authenticates the user based on their unique pattern behaviour such as how they type and move the mouse and touch screen (Debasis, 2022). This method is important in smart banking due to its ability to provide a continuous and non-intrusive authentication process.

a. **Benefits of Behavioural Biometric in smart banking**

i. It is very difficult for attackers to replicate this type of authentication. While usernames and passwords can be stolen or guessed, it is very hard to replicate the behavioural attribute of a user.

ii. ***Continuous authentication*:** The authentical method continuously monitors user behaviour throughout their session. This allows the detection of real-time potential threats. For example, if a user accessing their banking information leaves their computer unattended, attackers may try to take advantage of the situation to steal the user's sensitive information. In such a scenario, behavioural biometrics can detect the changes in the user's behaviour and prevent unauthorized access to the account.

3. ***Artificial Intelligence and machine learning***: AI and machine learning are important technologies that can be used to provide advanced security control for smart banking technology. These technologies can provide security controls like:

i. **Fraud detection and alert:** AI and ML algorithms can be used in smart banking to analyze transaction information to detect unusual patterns indicating possible fraudulent activities. The detection is done using historical data to identify the attack pattern. They can also adapt to new threats by learning from new data patterns. The algorithm can be configured to alert the user and bank about any unusual activity.

ii. **Phishing Detection:** AI and ML algorithms are important security controls that can detect phishing attacks by analysing the content of emails, text messages and website characteristics.

iii. **Virtual Assistance:** Chatbots can be developed in smart banking with AI algorithms to provide immediate assistance to bank users with security concerns and complaints. The system can be configured to give users advice, a security guide and steps to secure their accounts (Soni, 2019).

4. Blockchain technology

Blockchain technology is a global system that keeps records safely and clearly, that is both safe and clear. In the setting of smart banking, blockchain technology can be used to record financial events in a way that can't be changed. Blockchain technology can provide security controls like:

1. **Decentralization:** Through decentralization, blockchain eliminates the need for a central authority to manage and validate transactions. The controls make it very difficult for attackers to penetrate the system (Gan *et al*., 2021).
2. **Enhanced Security:** Blockchain uses the latest and most advanced cryptography algorithms for transaction protection. This makes it hard for attackers to steal sensitive information from the system (Osmani *et al*., 2021).
3. **Faster and more efficient:** The use of blockchain technology provides faster transactions by removing the need for intermediaries. This reduces the time and cost associated with traditional banking transactions (Gan *et al*., 2021)

REFERENCES

Nabi, A. U., Ahmed, M., & Abro, A. (2022). An overview of firewall types, technologies, and functionalities. *International Journal of Computing and Related Technologies*, *3*(1), 10-16.

Ahmed, Y. H. I., & Ibrahim, O. (2022). *EMV electronic payment system and its attacks: A review*. *Al-Rafidain Journal of Computer Sciences and Mathematics*, 16(1), 23–29.

Akinyokun, N., & Teague, V. (2017). *Security and privacy implications of NFC-enabled contactless payment systems*. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*.

Alam, M. U., Azad, M. A. K., & Ali, M. S. (2022). *Best practices to secure API implementations in core banking system (CBS) in banks*. In *Proceedings of the IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*.

Alhassan, A., & Ahmed, B. (2023). Social Engineering and Fraud Prevention in Digital Banking. Journal of Financial Cybersecurity, 8(2), 45–62.

Alzoubi, H. M., et al. (2022). *Cyber security threats on digital banking*. In *Proceedings of the 1st International Conference on AI in Cybersecurity (ICAIC)*.

Behbehani, D., Rajarajan, M., Komninos, N., & Al-Begain, K. (2022). *Detecting open banking API security threats using Bayesian attack graphs*. In *Proceedings of the 14th International Conference on Computational Intelligence and Communication Networks (CICN)*.

Benmoussa, M. (2019). *API "Application Programming Interface" banking: A promising future for financial institutions (international experience)*. *Revue des Sciences Commerciales*, 18(2), 31–34.

Bhasin, A., & Goyal, R. (2024). Machine Learning-Based Fraud Detection in Smart Banking. Computers & Security, 130, 103–118.

Bouveret, A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantification.* IMF Working Paper WP/18/143.

Carcillo, F., et al. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *IEEE Transactions on Neural Networks and Learning Systems*, 32(6), 2478–2490.

Chabbi, S., & Araar, C. (2022). *RFID and NFC authentication protocol for securing a payment transaction*. In *Proceedings of the 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*.

Chabbi, S., Madhoun, N. E., & Khamer, L. (2022). *Security of NFC banking transactions: Overview on attacks and solutions*. In *Proceedings of the 6th Cyber Security in Networking Conference (CSNet)*.

Chakraborty, D. S., & Debasis, S. S. (2022). *Fraudify: A secure open banking platform*. *International Journal of Scientific Research & Engineering Trends*, 8(1).

Chowdhury, M. M., Davis, D. K., & Rifat, N. (2022). *Password security: What are we doing wrong?* In *Proceedings of the IEEE International Conference on Electro Information Technology (eIT)*.

Churaev, I. L., Dakhkilgova, K. B., & Chaplaev, K. G. (2021). *NFC payment security*. In *ASE-I 2021: Applied Science and Engineering*.

Davis, D. K., Chowdhury, M. M., & Rifat, N. (2022, May). Password security: what are We doing wrong?. In *2022 IEEE International Conference on Electro Information Technology (eIT)* (pp. 562-567). IEEE.

European Union Agency for Cybersecurity (ENISA). (2023). *Threat Landscape for the Finance Sector.*

Financial Conduct Authority & Prudential Regulation Authority. (2021). *Operational Resilience: Impact Tolerances for Important Business Services* (Policy Statement PS21/3).

Gan, Q., Lau, R. Y. K., & Hong, J. (2021). *A critical review of blockchain applications to banking and finance: A qualitative thematic analysis approach*. *Technology Analysis & Strategic Management*, 1–17. https://doi.org/10.1080/09537325.2021.1979509

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). *A cyber-security culture framework for assessing organization readiness*. *Journal of Computer Information Systems*, 62(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). *Cyber security threats, vulnerabilities, and security solutions models in banking*. https://doi.org/10.22541/au.166385206.63311335/v1

Guers, K., Chowdhury, M. M., & Rifat, N. (2022). *Card skimming: A cybercrime by hackers*. In *Proceedings of the IEEE International Conference on Electro Information Technology (eIT)*.

Ifinedo, P. (2012). Understanding information security compliance in organizations: An integration of the Theory of Planned Behavior and Protection Motivation Theory. *Computers & Security*, 31(1), 83–95.

Jana, D. S., K., A. E., & K. C. E. (2021). *Importance of cyber security in banking*. *Vidyabharati International Interdisciplinary Research Journal*, 13(1), 203–206.

Karia, H., & Patel, S. (2022). Evaluating Multi-Factor Authentication in Mobile Banking Security. International Journal of Information Security, 21(4), 512–528.

Kassab, M., & Laplante, P. A. (2022). *Open banking: What it is, where it's at, and where it's going*. *Computer*, 55(1), 53–63. https://doi.org/10.1109/MC.2021.3108402

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic*.

Legowo, Y. J. N. (2022). *Risk assessment of information technology security system at a bank using ISO 27001*. *Journal of System and Management Sciences*, 12(3), 181–199. https://doi.org/10.33168/JSMS.2022.0310

Malinka, K., Hujnak, O., Hanacek, P., & Hellebrandt, L. (2022). *E-banking security study—10 years later*. *IEEE Access*, 10, 16681–16699. https://doi.org/10.1109/access.2022.3149475

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies. *Digital Threats Research and Practice*, 2(2), 1–20.

Mouha, N. (2021). *Review of the advanced encryption standard*. https://doi.org/10.6028/nist.IR.8319

Legowo, N., & Juhartoyo, Y. (2022). Risk management; risk assessment of information technology security system at bank using ISO 27001. *Journal of System and Management Sciences*, *12*(3), 181-199.

Nwankwo, C., & Okorie, I. (2021). *Security Governance and Organizational Resilience in Digital Banking. African Journal of Information Systems, 13(3), 89–105.*

Ogunniyi, P. (2023). *SCADA: Data management and risk analysis* (Master's thesis). Manchester Metropolitan University.

Osmani, M. E.-H., Hindi, R., Janssen, M., Weerakkody, V., & J. P., V. (2021). *Blockchain for next-generation services in banking and finance: Cost, benefit, risk and opportunity analysis*. *Journal of Enterprise Information Management*, 34(3), 884–899.

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to phishing using cognitive reflection and cyber security knowledge. *Computers in Human Behavior*, 99, 272–284.

Ponsard, C., & Massonet, P. (2022). *Survey and guidelines about learning cyber security risk assessment*. In *Proceedings of the 8th International Conference on Information Systems Security and Privacy*.

Rajabboyeva, X. O. U. S. B. q. (2023). *The necessity and benefit of multi-factor authentication*. *International Bulletin of Applied Science and Technology*, 3(4), 960–964. https://doi.org/10.5281/zenodo.7882398

Sharma, P., & Gupta, R. (2021). Cybersecurity challenges in digital banking: Threats, vulnerabilities, and mitigation strategies. *Journal of Financial Technology*, 6(3), 15–28.

Soewito, B., & Andhika, C. E. (2019). *Next-generation firewall for improving security in company and IoT network*. In *Proceedings of the 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)* (pp. 205–209). https://doi.org/10.1109/ISITIA.2019.8937145

Soni, V. D. (2019). Role of artificial intelligence in combating cyber threats in banking. *International Engineering Journal for Research & Development*, *4*(1), 7-7.

Sportiello, L. (2019). *Internet of smart cards: A pocket attacks scenario*. *International Journal of Critical Infrastructure Protection*, 26. https://doi.org/10.1016/j.ijcip.2019.05.005

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *37*, 100505.

Walter, S., & Narring, F. (2020). How can supervisors and banks promote a culture of strong governance and ethical behaviour?. *Journal of Risk Management in Financial Institutions*, *13*(2), 145-154.