Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 43-48
Published by *Majmuah Enterprise*
www.majmuah.com

Comparison of Security Measures in Online Banking Sector Malaysia

SUREN KRISHNAN[1] and MOHD KHAIRUDIN BIN KASIRAN[2]
[1]*Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA*
[2]*School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA*
Email: surenkrishnan12@yahoo.com , mkasiran@uum.edu.my | Tel: +601126532127, +60134318188 |

Received: July 28, 2023
Accepted: August 10, 2023
Online Published: September 01, 2023

Abstract

The banking sector plays a vital role in the economic growth of a country, as it serves as the backbone of financial transactions and services. With the progression of technology, the banking industry has observed significant transformations, accompanied by a risen risk of security breaches and cybercrimes. This research paper studies the security measures adopted by the banking sector in Malaysia to safeguard customer data, prevent fraud, and ensure the reliability of financial transactions. The research uses a combination of qualitative research methods and an examination of current security practices.

Keywords: security; measure; banking; technology; risk

1. Introduction

The banking sector in Malaysia is an essential component of the nation's economy, facilitating financial transactions, providing a range of financial services, and supporting economic growth. With the rapid developments in technology and the increasing reliance on digital platforms, the banking industry has undergone significant transformations. While these technological advancements have brought about numerous advantages, they have also introduced new risks and challenges, particularly in terms of security (Manoj, 2021). The safeguarding of customer data, prevention of fraudulent activities, and maintenance of the integrity of financial transactions are of utmost concern for the banking sector (AL-Hawamleh, 2023). Security breaches and cybercrimes pose substantial threats to both financial institutions and their customers. As a result, it is imperative for banks to implement security measures to safeguard sensitive information, maintain customer trust, and uphold the stability of the financial system (Bultum, 2014). Not only there are more cases of online banking fraud, but the sum of money being defrauded is also skyrocketing. Many Malaysians who have access to online banking are becoming more concerned about cybercrime. Malaysians have fallen victim to scams and lost around RM415 million in the first seven months of 2022.

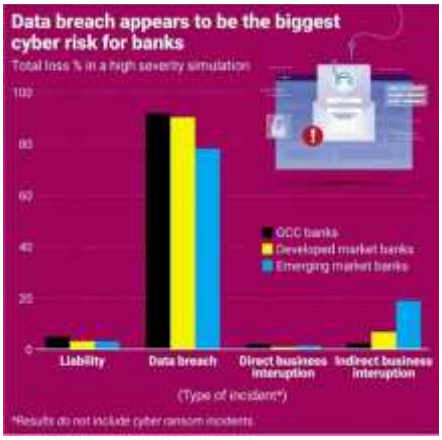

Figure 1: Statistics of data breach for banks (Nair, 2022)

The primary objective of this research paper is to explore the security measures implemented by the banking sector in Malaysia. By examining the strategies, technologies, and practices employed by banks, this study purposes to provide insights into the effectiveness of current security measures and identify areas for improvement. The research objectives include assessing the current security landscape in the banking sector in Malaysia, examining the security measures implemented by banks to protect customer data and prevent fraud.

This research paper utilizes a combination of qualitative research methods to investigate security measures in the banking sector in Malaysia. The study comprises an examination of existing security practices. The data gathered will be analyzed to acquire a comprehensive understanding of the security measures implemented by banks and to derive meaningful insights into the current state of banking security in Malaysia. By exploring the security measures in place and the challenges faced by banks, this research purposes to contribute to the body of knowledge regarding banking sector security and provide recommendations for improving security measures in the context of Malaysia.

2. Literature Review

2.1 Overview of the banking sector in Malaysia

The banking sector in Malaysia plays a vital role in the country's economic growth and stability. It comprises of various types of financial institutions, including commercial banks, Islamic banks, investment banks, and other specialized institutions (Yusof, Ahmad, & Mohamed, 2016). These institutions provide an extensive range of financial services, such as deposit-taking, lending, fund management, and payment systems. In recent years, the banking sector has witnessed significant technological advancements and the expanding adoption of digital banking services. This shift towards digital platforms has brought various benefits, including convenience, accessibility, and efficiency. However, it has also introduced new security challenges and risks.

The changing threat landscape poses substantial risks to the security of the banking sector in Malaysia. Cybercriminals endlessly develop sophisticated techniques to exploit vulnerabilities and gain unauthorized access to sensitive information. Some of the important threats faced by the banking sector include phishing attacks, where malicious actors try to deceive individuals into revealing sensitive information, which remains a substantial concern (Yazdanifard, WanYusoff, Behora, & Sade, 2011). Social engineering techniques, such as impersonation and manipulation, are generally employed to trick individuals into divulging confidential data. Insider threats, whether intentional or unintentional, pose a considerable risk. Employees with privileged access to banking systems may misuse their privileges, leading to data breaches or financial fraud. Insufficient security controls and inadequate employee awareness can exacerbate these risks (Khanna & Arora, 2009). The banking sector holds huge amounts of sensitive customer data. Data breaches, either through external attacks or internal vulnerabilities, can result in the exposure of personal and financial information. This can lead to financial losses, identity theft, and reputational damage for both banks and customers. The proliferation of malware and ransomware presents a significant threat to the banking sector. These malicious software programs can infiltrate banking systems, compromise data integrity, and disrupt operations (Geramiparvar & Modiri, 2015). Ransomware attacks particularly target financial institutions to extort money by encrypting critical data.

2.2 Regulatory frameworks and guidelines

To address the security challenges faced by the banking sector, regulatory frameworks and guidelines have been established in Malaysia. The Central Bank of Malaysia (Bank Negara Malaysia) serves as the core regulator and has issued guidelines and regulations to ensure the security and resilience of the banking system (Musa, 2015). Guidelines on Risk Management in Technology (RMiT) outline the expectations for banks to establish robust technology risk management frameworks, including security measures, incident response plans, and regular risk assessments (Risk Management in Technology (RMiT), 2020). The Personal Data Protection Act (PDPA) governs the collection, storage, and processing of personal data in Malaysia. It insists on banks to implement appropriate security measures to safeguard customer data and obtain consent for data usage (Yusof, Ahmad, & Mohamed, 2016). Bank Negara Malaysia has developed a comprehensive cybersecurity framework that provides guidance to banks on managing cyber risks efficiently.

The framework encompasses areas such as governance, risk management, and incident response. The banking sector in Malaysia is also subject to stringent Anti-Money Laundering and Counter Financing of Terrorism regulations to avoid illicit activities. These measures include customer due diligence, transaction monitoring, and reporting suspicious activities (Yazdanifard, WanYusoff, Behora, & Sade, 2011). The regulatory frameworks and guidelines play an essential role in shaping the security landscape of the banking sector in Malaysia. They establish standards, promote best practices, and encourage banks to adopt robust security measures to mitigate risks and protect stakeholders' interests. Overall, the banking sector in Malaysia faces a dynamic and evolving security landscape. The emergence of new threats and the increasing reliance on technology necessitate constant vigilance and proactive security measures to safeguard customer data, prevent fraud, and retain the trust and stability of the financial system.

3. Security measures in the banking sector

3.1 Role of technology in the banking sector

Technology has revolutionized the banking sector, offering unprecedented convenience, efficiency, and access to financial services. However, the widespread adoption of technology also introduces new security challenges that banks must address. Understanding the role of technology in banking security is essential for implementing effective security measures. Online banking platforms and mobile applications have become ubiquitous in the banking industry. They enable customers to perform a wide range of transactions, including fund transfers, bill payments, and account management (Sharma & Sharma, 2013). However, the security of these platforms is critical to protect sensitive customer data and prevent unauthorized access. With the growth of digital payments, the banking sector has seen an increase in the use of payment systems and e-wallets (Teoh Teng Tenk, Yew, & Heang, 2020). These technologies offer convenient and contactless transactions. Ensuring the security of these systems is crucial to protect against fraudulent activities and unauthorized transactions.

3.2 Security measures in the online banking sector

The online banking sector in Malaysia implements several authentication and access control measures to ensure the security of user accounts and protect against unauthorized access. Here are some common security measures used in the online banking sector in Malaysia.

User ID and Password: Customers are required to create unique user IDs and strong passwords during the registration process. These credentials serve as the primary authentication method to access their online banking accounts (Sinigaglia, Carbone, Costa, & Zannone, 2020). Two-Factor Authentication (2FA): Many banks in Malaysia have implemented 2FA to add an extra layer of security. This involves using a secondary authentication method, such as One-Time Passwords (OTP) sent via SMS or generated by mobile apps, to verify the user's identity during login or certain transactions (Sinigaglia, Carbone, Costa, & Zannone, 2020).

Multi-factor authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple pieces of evidence to verify their identity. This may include a combination of passwords, security tokens, biometrics, or one-time passcodes. MFA enhances the security of customer logins, preventing unauthorized access to accounts (Sinigaglia, Carbone, Costa, & Zannone, 2020).

Security Tokens: Some banks provide customers with physical security tokens or virtual security token apps. These tokens generate unique authentication codes that are required during login or for specific transactions, adding an additional layer of security (Sinigaglia, Carbone, Costa, & Zannone, 2020).

Biometric Authentication: Biometric authentication methods, such as fingerprint scans and facial recognition, have gained prominence in banking security. These technologies provide an additional layer of security by verifying the user's unique physiological or behavioral traits. Biometric authentication enhances the security of transactions and reduces the reliance on traditional password-based authentication (Hammood, et al., 2020).

Session Timeout: To prevent unauthorized access due to inactivity, online banking sessions are automatically logged out after a certain period of inactivity. This reduces the risk of someone gaining access to an active session if the user forgets to log out (Al-Thobhani, 2020).

4. Data Collection and Analysis

The findings from the case study will be presented in a comprehensive manner, highlighting the security measures and practices implemented by the selected banks. The analysis will shed light on the effectiveness of these measures in addressing security risks and safeguarding customer data. The findings may include examination of multi-factor authentication methods, user access controls, and identity verification procedures employed by the banks. The findings will provide a comprehensive understanding of the security measures adopted by Malaysian banks, their strengths, and areas that may require improvement. These insights will contribute to enhancing security practices in the banking sector and inform recommendations for further strengthening security measures.

Table 1: Website

Bank	**Viewing account**	**Transfer**
A	Password	Password & secure2u
B	Password	Password & secureTAC
C	Password	Password & OTP
D	Password	Password & APPAuthorise
E	Password	Password & isecure authentication

Table 2: Mobile Application

Bank	**Viewing account**	**Transfer**
A	PIN/Password/Biometric	Biometric & password & secure2u
B	Biometric & Password	Biometric & password & secureTAC
C	Password/Biometric	Password & OTP
D	Password/Biometric	Biometric & password & APPAuthorise
E	Password/Biometric	Biometric & password & isecure authentication

5. Challenges and Future Directions

The While technology-based security measures offer substantial benefits, implementing and retaining them presents various challenges for banks. The rapid pace of technological developments makes it challenging for banks to keep up with advancing security threats and adopt appropriate security resolutions. Implementing complex security technologies involves specialized knowledge, resources, and ongoing updates to stay ahead of emerging risks. Balancing security with user experience and convenience is a challenge for banks. Uncompromising security measures, such as multi-factor authentication, might increase friction and inconvenience for consumers (Sinigaglia, Carbone, Costa, & Zannone, 2020). Banks must find a balance that guarantees strong security without compromising the user experience. Regardless of robust security measures, insider threats remain a crucial challenge. Insiders with authorized access to systems and data can intentionally or unintentionally compromise security. Banks need to implement stringent access controls, employee monitoring, and awareness programs to reduce insider threats.

Banks must comply with a multitude of regulatory requirements related to privacy, data protection, and security. Ensuring compliance with these regulations while continuing effective security measures can be complex and resource intensive (AL-Hawamleh, 2023). As technology develops, new security threats and vulnerabilities constantly emerge. Banks must stay vigilant and proactive in detecting and addressing these emerging threats to make sure the security of their systems, applications, and customer data. To address these challenges, banks must constantly invest in security technologies, keep alongside of the latest threats and trends, conduct consistent risk assessments, and foster a strong security culture within their organizations. Technology plays a crucial role in the banking sector, enabling developed services and convenience. However, it also introduces security challenges that banks must address. By leveraging appropriate security technologies and solutions and addressing the correlated challenges, banks can strengthen their security posture and deliver customers with a secure and trusted banking experience (Al-Thobhani, 2020).

6. Conclusion

The banking sector in Malaysia works in an environment where security is of dominant importance. As technology continues to advance and the threat landscape evolves, banks must remain cautious in implementing security measures to safeguard customer data, prevent fraud, and ensure the integrity of financial transactions. This research paper has studied the security measures in the Malaysian banking sector, including the security landscape, technology and banking security. The security landscape analysis revealed the expanding complexity and sophistication of security threats faced by banks. With the hike of digital banking, the adoption of technology-based solutions, and the growing reliance on online and mobile platforms, banks are encountering with new challenges. However, it was evident that banks have recognized the importance of implementing comprehensive security measures to safeguard their systems and customer information.

The role of technology in banking security was explored, emphasizing the essential role of online banking platforms, mobile apps, payment systems, and biometric authentication. These technologies present convenience and efficiency to customers but also require robust security measures to safeguard against unauthorized access and fraudulent activities. The case study on security measures in Malaysian banks provided valuable insights into the security practices and measures adopted by selected banks. The findings emphasized the importance placed on online security, data protection, authentication, and access control. The case study demonstrated that banks in Malaysia have implemented various security technologies and practices to mitigate risks and safeguard customer information. However, it is essential to acknowledge the challenges that banks face in implementing robust security measures. The rapidly developing threat landscape, limited resources and budget, complex regulatory landscape, human factor, and the necessity to balance security and user experience were identified as key challenges. These challenges require constant efforts and investments to overcome and ensure the effectiveness of security measures.

Looking towards the future, several directions were recommended to enhance security measures in the banking sector. These include the adoption of advanced technologies, collaborative threat intelligence sharing, continuous security monitoring, security culture and employee awareness, and integrating security into digital transformation initiatives. By adopting these future directions, banks can strengthen their security posture and effectively address emerging threats. In conclusion, the security measures implemented by Malaysian banks in the face of evolving security challenges demonstrate their commitment to safeguarding customer data and ensuring secure financial transactions. By constantly assessing the security landscape, leveraging advanced technologies, and fostering a strong security culture, banks in Malaysia can continue a robust security posture and uphold the trust and faith of their customers.

References

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. . International Journal of Advanced Computer Science and Applications, 12, 801-809.

Al-Thobhani, N. S. (2020, February). Building A Secure Internet Banking Environment for The Bank.

Bultum, A. G. (2014, June). Factors Affecting Adoption of Electronic Banking System in Ethiopian. Journal of Management Information System and E-commerce, 1(1), 1-17.

Geramiparvar, S., & Modiri, N. (2015, March). Security as a Serious Challenge for E-Banking: a Review of Emmental Malware. International Journal of Advanced Computer Research, 5(18), 62-67.

Hammood, W. A., Abdullah, R., Hammood, O. A., Asmara, S. M., Al-Sharafi, M. A., & Hasan, A. M. (2020, February). A review of user authentication model for online banking system based on mobile IMEI number. In IOP Conference Series: Materials Science and Engineering, 769(1), 012061.

Khanna, A., & Arora, B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry. International Journal of Business Science & Applied Management (IJBSAM), 4(3), 1-21.

Manoj, K. S. (2021, January). Cyber risk in banking services: the extent of cyber risks provisions and security measures. International Journal of Management (IJM), 12(1), 1332-1339.

Musa, M. A. (2015). The role of Bank Negara Malaysia in limiting imprudent consumption. Intellectual Discourse, 475-494.

Nair, K. (2022, 10 01). The rise of online financial fraud in Malaysia. Retrieved from TheStar: https://www.thestar.com.my/business/business-news/2022/10/01/the-rise-of-online-financial-fraud-in-malaysia

Risk Management in Technology (RMiT). (2020, June). Retrieved from https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078

Sharma, M. C., & Sharma, A. (2013). Role of information technology in indian banking sector. International Journal in Multidisciplinary and Academic Research, 2(1), 1-12.

Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020, August). A survey on multi-factor authentication for online banking in the wild. Computers & Security, 95, 101745.

Teoh Teng Tenk, M., Yew, H. C., & Heang, L. T. (2020). E-wallet Adoption: A case in Malaysia. International Journal of Research In Commerce and Management Studies, 2(2), 216-233.

Yazdanifard, R., WanYusoff, W. F., Behora, A. C., & Sade, A. B. (2011). Electronic banking fraud: The need to enhance security and customer trust in online banking. International Journal in Advances in Information Sciences and Service Sciences , 3(10), 505-509.

Yusof, N. M., Ahmad, N. A., & Mohamed, Z. (2016). A Study on Collection of Personal Data by Banking Industry in Malaysia. Journal of Advanced Research in Business and Management Studies, 2(1), 39-49.