Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

INTEGRATING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: A CASE STUDY OF MAYBANK'S INFORMATION SECURITY STRATEGY

Intan Nurul'Ain Mohd Firdaus Kozako[1]
Lai See May[2]
Siti Norhana Shahira Rumi[3]
Nurul Syazana Aliah Rosli[4]
Intan Masnita Azhar[5]
Nor Anis Ghazali[6]

[1]Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia, (E-mail: intan866@uum.edu.my)
[2]Academy of Language Studies, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia, (E-mail: laiseemay@uitm.edu.my)
[3]Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia, (E-mail: 2022898854@student.uitm.edu.my)
[4]Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia, (E-mail: 2022835762@student.uitm.edu.my)
[5]Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia, (E-mail: 2022675094@student.uitm.edu.my)
[6]Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia, (E-mail: 2022850604@student.uitm.edu.my)

Article history
Received date : 11-7-2025
Revised date : 12-7-2025
Accepted date : 7-9-2025
Published date : 25-9-2025

To cite this document:
Mohd Firdaus Kozako, I. N., May, L. S., Rumi, S. N. S., Rosli, N. S. A., Azhar, I. M., & Ghazali, N. A. (2025). Integrating artificial intelligence in cybersecurity: A case study of Maybank's information security strategy. *Journal of Islamic, Social, Economics and Development (JISED),* 10 (76), 720 – 732.

Abstract: *This study demonstrates how Maybank's integration of Artificial Intelligence into its cybersecurity framework illustrates both the opportunities and challenges of adopting advanced technologies in the banking sector. By applying machine learning algorithms and real-time analytics, Maybank has strengthened its capabilities in threat detection, fraud prevention, and proactive risk management, while reinforcing customer trust and regulatory compliance. However, the findings also reveal persistent obstacles, including high implementation costs, false positives, shortages of skilled professionals, and growing data privacy concerns. The case highlights the importance of a hybrid approach in which AI systems work in tandem with human expertise to ensure accuracy, accountability, and resilience against evolving threats. Importantly, this research addresses a gap in the literature by providing one of the first Southeast Asian case studies on AI-enabled cybersecurity in banking. The insights generated here offer practical implications for financial institutions seeking to balance innovation, regulatory demands, and operational challenges in dynamic digital ecosystems.*

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

Keywords: *Artificial Intelligence, Cybersecurity, Banking Sector, Maybank, Threat Detection*

Introduction

Artificial Intelligence (AI) play a very significant role in cybersecurity today particularly within financial institutions. As cyber threats evolve in complexity and frequency, organizations such as Maybank, a leading bank in Southeast Asia are leveraging AI to enhance information security, prevent fraud, and maintain customer trust. AI is useful for the organisation because it has the capability to facilitate predictive threat analysis, real-time monitoring, and data-driven risk management. However, deploying such technologies also introduces new ethical, regulatory, and operational challenges to the organisation. Hence, this study intends to explore how Maybank, one of the leading banks in the industry embraces AI to strengthen its cybersecurity efforts. It also explores how successful this journey has been and what the future might look like as the bank continues to protect its customers and data through continuos innovations.

Malayan Banking Berhad (Maybank), founded in 1960, is Malaysia's largest financial institution and a key player in Southeast Asia. As a major financial institution, it is a prime target for increasingly sophisticated cyberattacks. While AI is widely promoted as a solution for real-time threat detection and fraud prevention, its implementation in the banking sector is hindered by high costs, shortage of skilled professionals, and data privacy concerns. Despite growing global research on AI in cybersecurity, there remains a lack of case studies focusing on Southeast Asia, particularly Malaysia. This study fills that gap by examining how Maybank integrates AI into its cybersecurity framework, the challenges it faces, and the lessons it offers for the regional banking industry.

The banking and finance industry often needs to deal with a huge number of sensitive financial data and transactions. As a result of so, they have placed themselves in a very high-risk situation where they might be attacked by the irresponsible cybercriminals anytime anywhere. Hence, as a prominent player in the banking industry, it is vital for Maybank to recognise the essential of staying ahead of these emerging cyber threats to protect its operations and safeguard customer assets. Maybank has been very proactive by taking different initiatives to invenst in advanced technologies. One of the initiatives taken by Maybank is the use of Artificial Intelligence (AI) in its opetaion to improve its information cybersecurity system. The assistance of AI-driven solutions has allowed Maybank to identify and mitigate threats proactively to ensure the integrity and reliability of its digital platforms. As a result of the smart use of AI, Maybank's AI cybersecurity system secures its operations and strengthens its reliability by earning trust among its customers and stakeholders. This makes Maybank a great example among the industry players of how the industry can utilise AI in their operation to enhance and upscale their cybersecurity.

AI is a comprehensive approach in comprehending, simulating, and producing intelligence in its many forms. It is a crucial field in cognitive science, and the humanities are now beginning to feel the effects of it increasingly. One definition of intelligence is the capacity to acquire and use appropriate methods to solve issues and accomplish objectives in a world that is unpredictable and constantly changing. Emeritus Stanford Professor John McCarthy in 1955

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

said AI was defined as “the science and engineering of making intelligent machines” (Wahab, 2024).

According to Gautam et al. (2024), cybersecurity serves as a critical safeguard for digital devices such as smartphones and computers, protecting them from sophisticated cyber threats. It involves the implementation of advanced security protocols and technologies designed to defend digital assets against malicious software, unauthorized access, and cyberattacks. Much like physical security measures used to protect homes, cybersecurity operates as a vigilant system that continuously monitors online activity, assesses potential threats, and promotes cautious behavior such as verifying email sources and securing sensitive data to ensure the integrity and confidentiality of digital environments.

Futhermore, AI has become more relevant these days, considering modern businesses and their ever-growing dependency on digital platforms. With the ever-increasing volume of online transactions, cloud computing, and work-from-home engagement, new avenues seem to be opening every day for the cyber thief to explore weaknesses in systems. That is how AI can come into use like identification of new threats at higher speeds, incident response, and even threat anticipation. This would further help in reducing human error, automation of mundane tasks, and freeing the security teams to focus on higher-value problems.

For such organizations, investment in artificial intelligence-powered cybersecurity is neither only a safety issue but rather of continued customer confidence and assured success in the long term especially business like banks such as Maybank. AI and cybersecurity just happened to connect more than ever in this digital world of ours. The more innovative it all turns for users around the world, the bigger the need for smart and proactive security solutions will develop. With AI inbuilt inside cybersecurity, businesses can definitely ensure better protection against rapidly evolving threats and that digital infrastructures are strong, safe, and trustworthy.

Literature Review

The banking industry has become increasingly reliant on digital infrastructure, making information security (infosec) a critical priority. Financial institutions handle vast amounts of sensitive data, including personal customer information and transactional records, which are prime targets for cybercriminals (Abu-Mostafa et al., 2022). Traditional infosec measures, such as firewalls and encryption, are no longer sufficient to combat sophisticated cyber threats like advanced persistent threats (APTs), ransomware, and social engineering attacks (Kumar et al., 2023). As a result, banks are turning to AI to enhance their cybersecurity frameworks. AI offers advanced capabilities such as real-time anomaly detection, predictive analytics, and automated response systems, which significantly improve threat identification and mitigation (Lee & Park, 2023).

Whether in the context of the banking sector with its overriding focus on speed and accuracy or data security in general, practitioners believe that realising AI's true potential will require a paradigm shift. AI encompasses Machine Learning (ML), wherein ML algorithms examine patterns potentially linked to cybersecurity breaches by using both historical and real-time data. For instance, the AI-based systems can identify abnormal transaction activity that is indicative of fraud and thus reducing false negatives by 40 percent (Nguyen et al., 2023). Moreover, various AI approaches such as Natural Language Processing (NLP) are utilized to monitor and

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

analyze communication media channels for phishing and social engineering activities (Zhang et al., 2024). Such technologies help banks like Maybank to be able to pre-empt threats even before too much damage is done. AI also works to improve operational efficiency by removing the burden of repetitive security-related tasks from human analysts and allowing them to concentrate on the complex threats that demand judgment and context (IBM Security, 2023).

Although AI offers a huge number of advantages in banking cybersecurity, it is undeniable that it also comes with major challenges. One major issue is the high cost of implementation and maintenance. Setting up steady and stable AI systems require huge amount of investments in terms of infrastructure, software, and skilled personnel, which might cost more than $2 million for large institutions as stated in World Economic Forum (2023). Besides, prevalence of false positives is also one challenge that need to be tackled by the organisation. This happens when legitimate activities are mistakenly flagged as threats. It strains resources and risks eroding customer trust if transactions are unnecessarily blocked (Patel & Smith, 2023). In addition, data privacy is another critical issue that should be given extra concern, as AI systems rely on vast datasets that may include sensitive customer information. This brings uo the concerns on how the data can be effectively protected. Therefore, banks must strictly adhere to rules and regulations such as the General Data Protection Regulation (GDPR) and Malaysia's Personal Data Protection Act (PDPA). These laws add layers of complexity for banks to access their customers' personal data, requiring them to balance innovation with legal and ethical considerations (European Union Agency for Cybersecurity, 2021).

The dynamic nature of cyber threats has made it more difficult and complicated to banks to invent a good AI for the purpose of cybersecurity. Cybercriminals are increasingly using AI themselves to develop more sophisticated attacks, creating an arms race where the defenders (banks) and the attacker are trying to battle with each other by applying a more advanced system using AI (Bank for International Settlements, 2022). For instance, hackers use adversarial AI techniques to trick Machine Learning (ML) models by feeding them manipulated data. This causes the system to process and analyse incorrect data which eventually cause threat assessments (Abu-Mostafa et al., 2022). Additionally, the shortage of professionals skilled in both AI and cybersecurity poses a barrier to effective implementation of AI cybersecurity in the banking industry. Therefore, banks must invest in continuous training and collaboration with academic institutions to bridge this gap by building up ample number of talents in this particular area of AI cybersecurity (Malaysia Digital Economy Corporation, 2022).

Recent research shows that AI plays a very significant role in cybersecurity. AI in cybersecurity allows automating threat detection, improving anomaly recognition, and enabling predictive analytics (Johnson & Patel, 2023; Liu & Chen, 2023). In the financial sector, AI is effective in tracking and checking transactional data for fraud, a trend increasingly adopted by major institutions (Smith, 2023; Wahab, 2024). Challenges such as algorithmic bias, data privacy, and explainability of AI decisions have been widely discussed (Miller, 2022; World Economic Forum, 2022). Human-AI collaboration is emphasized as a hybrid model that enhances overall cybersecurity performance (Nik Sharmine, 2024). Additionally, new technological frontiers like federated learning and quantum computing are poised to redefine AI's role in data protection (Kumar et al., 2023; Zhang & Li, 2022). However, while many studies highlight AI's theoretical contributions to cybersecurity, few provide empirical analysis

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

of how banks in Southeast Asia operationalize AI-driven systems. This study contributes to filling this gap by providing a detailed case analysis of Maybank.

Factors Contributing to the Need for AI in Cybersecurity

The increasing frequency and sophistication of cyber threats pose significant challenges to the financial services industry, particularly in high-stakes environments where sensitive customer data and large-scale transactions are managed daily (Gautam et al., 2024; Wahab, 2024). Traditional cybersecurity measures, while foundational, often lack the speed, adaptability, and predictive capabilities required to respond effectively to modern attack vectors such as phishing, ransomware, and insider threats (Miller, 2022; Johnson & Patel, 2023). In response, Artificial Intelligence (AI) has emerged as a pivotal technological solution, enabling real-time threat detection, automated incident response, and behavior-based fraud prevention (Liu & Chen, 2023; Smith, 2023).

However, the integration of AI into cybersecurity systems is not without challenges. Financial institutions face high implementation costs, limited availability of skilled AI professionals, regulatory constraints, and ethical concerns related to data privacy and algorithmic decision-making (Zhang & Li, 2022; Ahmed & Lee, 2023). Moreover, while global studies have explored AI's theoretical and technical contributions to cybersecurity, there remains a lack of empirical evidence detailing how AI is operationalized within specific organizational contexts in Southeast Asia, particularly in Malaysia.

Methodology

This case study adopts a qualitative research approach. Primary data was obtained through semi-structured interviews with Maybank's cybersecurity personnel, while secondary data was collected from recent scholarly articles, white papers, and official publications. Thematic analysis was used to identify key patterns and issues in the integration of AI into cybersecurity frameworks. Ethical considerations included anonymization of personal data and adherence to academic standards for secondary data usage.

Findings and Discussion

Security Threats and AI Tools

The interview indicates that Maybank use AI as its primary instrument for cybersecurity and fraud prevention strategies. This is a method to guarantee the security of its digital platforms and consumer transactions. A significant use of AI observable in banking is threat detection. This system employs advanced machine learning algorithms to identify and mitigate possible cyber risks such as phishing attempts, ransomware attacks, and other malicious actions. These AI-driven solutions can continually monitor network traffic and user behaviour to detect any anomalous behaviours. The capacity to recognise potential hazards at an early stage is crucial, as it enables the bank to respond swiftly and efficiently, therefore mitigating potential damages.

In addition to threat detection, Maybank also employs AI to strengthen its fraud prevention efforts. AI tools can detect abnormal or unusual activities that may be a sign or a warning of fraudulent activities, such as unauthorized account access, unusual spending habits, or identity theft attempts by analyzing transaction patterns in real-time. These systems, generated by AI, can process large volumes of data in milliseconds. This allows the bank to flag and block

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

suspicious transactions before they are finalized by the potential criminals. This proactive approach is significantly useful in protecting customers and boosting the bank's operational efficiency for its outstanding ability to decrease the need for monitoring the accounts manually.

Moreover, the AI cybersecurity tools used in Maybank is not merely limited for threats detections. The AI tools are also meant to learn from new data to help them to be more effective and efficient in combating cyber criminals that keep evolving day to day. By integrating AI into its security framework, Maybank shows its dedication to using cutting-edge technology to protect its assets and maintain customer trust. This incorporation of AI into its cybersecurity strategy positions the bank as a frontrunner in embracing innovative solutions to tackle modern digital challenges.

AI's Role in Threat Detection

As for the threat detection, Maybank uses AI to deal with threat incidences in response mechanisms is rightly detection for the bank. The AI forms the core of quick detection and response to emerging threats by analyzing huge amounts of data ranging from network traffic, customer transactions to system logs. This real-time processing of data by AI-driven systems helps identify any aberrant patterns or activities within those data streams, which include unauthorized access or fraudulent transactions that hint at security breaches. Machine learning techniques are used in bank systems so that they learn from the data of earlier times to adapt to the new evolving threats and predict the risks looming in the future.

Meanwhile, the continuous monitoring and analysis of data without human intervention is the most significant benefit of AI in threat detection. It includes out-of-the-norm behaviors such as alteration in customer behavior, which an individual would have a problem detecting with ease or may take longer to verify. If customer activity deviates from its normal pattern, AI can always demonstrate that transactions have occurred in an unusual or inconsistent way with previous spending behaviors. There are security breach defenses that flag such activities and put alarms to the security teams for probing and the bank can introduce deterrent measures. Cyber threats are continuously evolving, and thus AI helps Maybank in changing and enhancing its security systems to stay one step ahead of threats.

Challenges in AI Adoption

AI has given a lot of benefit to the business, but Maybank faces several challenges in adopting these advanced technologies. Based on the interview, one of the primary issues is the lack of specialized expertise required to implement and manage AI systems. Those used in cybersecurity require professionals who are not only skilled in AI but also in understanding complex cybersecurity landscapes and high cost associated with implementing and maintaining AI-driven cybersecurity solutions. Finding and retaining talent with the right combination of skills in both AI and cybersecurity has proven to be another challenge for Maybank and this shortage of skilled workers can slow down the adoption process.

Other challenges Maybank faced is the occurrence of false positives, where legitimate activities are mistakenly flagged as security threats. While AI systems are designed to learn and improve over time, the risk of false alarms remains an issue. AI systems can only make decisions based on patterns and data and they lack the contextual understanding of human security that lead to these false positives of creating unnecessary workload for the security team, leading to time

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

spent investigating non-issues rather than focusing on actual threats. This challenge requires continuous refinement of AI models to balance sensitivity and accuracy.

Human-AI Collaboration

Human intervention is still necessary for certain security such as Maybank's MAE (Maybank Anytime Everyone) application (Nik Sharmine, 2024). The application is designed for seamless banking, it does utilize AI to enhance customer experience, but it is not entirely based 100 percent on AI. The app incorporates AI for certain features, such as chatbots; such as MAE's virtual assistant, personalized financial recommendations, and fraud detection, which are powered by machine learning algorithms. However, it still relies on a combination of traditional banking systems, human intervention, and other technologies to function effectively as it showcases how AI and human professionals work together to enhance the banking experience.

The MAE app uses AI for various functions like personalized financial recommendations, fraud detection, and virtual assistants (chatbots). AI is very useful when it comes to handling routine tasks, analysing user data, and providing immediate responses to common queries. However, although AI can handle many basic interactions, it cannot handle everything. Thus, human intervention is still necessary for complex situations like resolving disputes, handling high-value transactions, or offering specialised financial advice. The integration of AI allows human staff to focus on higher-level tasks to improve the efficiency of the overall process in the operation of the organisation. The combination of AI automation and human expertise is what makes the MAE app a great example of human-AI collaboration for operational efficiency. AI systems focus on routine processes, while humans provide oversight and address issues requiring judgment or specialized knowledge. This shows that teamwork between AI and the human can provide better service and smarter banking.

Impact on Security Strategy

The integration of AI has allowed Maybank to improve and improvise its information security and risk management. AI techniques are very effective in helping Maybank to improve real-time monitoring and threat identification. These two elements are crucial when it comes to addressing the growing complexity of cyberattacks that are getting more complex and complecated day by day. Machine learning algorithms and other AI-powered systems help to analyse enormous amounts of data to find trends, spot irregularities, and react to any breaches more quickly as compared to conventional techniques. This has helped the bank to reduce the damage that might occur because of unpredictable cyber threats. However, using AI in the banking cybersecurity always comes together with some challenges. Hence, to effectively leverage the potential of AI while addressing its limitations, Maybank should make some modification and impeovement to its traditional security approach. The bank should not be over-dependent to the technology, namely the AI. This is to make sure that AI can intergrate well with the current system and it helps yje bank to achieve the organisation’s goal. Additionally, developing a strong security strategy also requires addressing the ethical ramifications of automated decision-making and educating staff on how to work together with AI tools.

However, the alteration in risk management protocols significantly impacts outcomes. AI enables predictive risk assessments by analysing previous data to estimate future risks. Maybank has successfully implemented a more responsive and dynamic risk management

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

strategy due to these characteristics. To ensure precision and pertinence, it necessitates regular audits and continuous adjustments to AI models, underscoring the importance of human supervision in mitigating potential biases and errors in AI-generated insights. Due to the adaptability and scalability of AI systems, Maybank must be vigilant against emerging attacks that exploit inherent vulnerabilities in AI.

AI and Privacy Concerns

When it comes to resolving data privacy issues, Maybank's usage of AI capabilities presents both benefits and drawbacks. For AI-driven systems to work efficiently, they need access to enormous volumes of sensitive data. This situation raises questions regarding compliance with laws like the General Data Protection Regulation (GDPR) of the European Union and Malaysia's Personal Data Protection Act (PDPA). To preserve its reputation and adhere to the law, Maybank must carefully find a balance to ensure the AI technologies that they are using can also work well in protecting consumer privacy while analyzing the data. AI systems can recognise and notify users of unusual and questionable patterns of behavior that may lead them to detect possible data breaches. By automating the implementation of privacy policies and proactively correcting vulnerabilities, these solutions can help to improve and safeguard the security of consumers' information. However, if AI systems' massive data collecting and processing requirements are not adequately safeguarded, they may lead to vulnerabilities that unintentionally expose private data.

Maintaining accountability and openness in AI-driven decision-making processes is another difficulty Maybank faces. Clarity about the processing and use of personal data by AI tools is demanded by customers and regulatory agencies. Maybank invests in explainable AI solutions that offer insights into decision-making processes, conducts frequent audits, and enforces stringent access controls to solve this. In addition to reaffirming compliance, these actions foster trust with clients who are growing more worried about the privacy implications of AI technologies. Maybank also needs to handle the ethical issues surrounding AI and data privacy. The possibility of unforeseen outcomes, including algorithmic biases or data exploitation, becomes a serious concern as AI systems get more complex. Maybank seeks to achieve a balance between innovation and accountability by promoting a culture of moral AI practices and interacting with stakeholders to resolve privacy issues.

Future Developments

Maybank is being ready for upcoming developments in artificial intelligence capabilities that could further transform information security. New technologies that enable AI systems to learn from decentralized data without the need for direct data exchange, such federated learning, provide answers to privacy issues. The bank's capacity to protect sensitive client data while abiding by strict privacy laws could be greatly improved by this invention.

It is anticipated that Maybank's future security strategy would heavily rely on predictive analytics and adaptive learning systems. Through learning from changing attack patterns and modifying countermeasures appropriately, these tools will make it possible to detect threats with more sophistication. AI technologies, for example, might be able to anticipate any weaknesses before they are taken advantage of, enabling Maybank to take preventative action. But these technologies' growing complexity necessitates constant infrastructure spending, staff development, and cooperation with cybersecurity professionals.

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

Furthermore, the function of AI in cybersecurity may be impacted by developments in quantum computing. Although quantum technologies present chances for improved encryption, they also present new risks since hackers may use them to crack more conventional encryption techniques. Maybank invests in quantum-resistant encryption technologies and cultivates a culture of constant innovation and awareness because it understands how important it is to stay ahead in this quickly changing environment.

In the future, Maybank hopes to use AI developments to fortify its security ecosystem while resolving any obstacles. It is anticipated that the combination of biometric authentication and AI-powered behavioral analytics will further improve consumer safety. However, Maybank's capacity to continue taking an innovative and flexible approach to cybersecurity will determine how well these solutions perform. To create creative solutions and reduce the hazards connected with new AI technologies, cooperation between academic institutions, industry leaders, and regulators will be essential.

All things considered, Maybank has both opportunities and challenges because of the growth and integration of AI tools in information security. Although these tools improve the bank's capacity to identify and neutralize threats, they also necessitate cautious handling to handle privacy issues, moral dilemmas, and the constantly changing nature of cybersecurity threats.

Conclusion

Maybank’s integration of AI into its cybersecurity framework demonstrates how AI can be a powerful tool in fighting against modern cyber threats. The bank adopts advanced machine learning algorithms and real-time analytics to enhance its threat detection, fraud prevention, and overall risk management. These AI systems help to improve and upgrade the operational efficiency and at the same time, they are also able to contribute to customer trust and ensure the bank always comply the regulations set by the authorities. This study extends current literature by providing one of the first case-based analyses of AI integration in cybersecurity within Southeast Asia. By focusing on Maybank, it demonstrates both the opportunities and barriers of AI deployment in a regional banking context, contributing to a clearer understanding of how financial institutions can navigate skills shortages, high implementation costs, and privacy regulations while remaining resilient to evolving cyber threats.

On the other hand, the use of AI un cybersecurity is unavoidable from its challenges. Setting up and running AI system can demand high operational costs. At the same time, the prevalence of false positives, and the shortage of AI-literate cybersecurity professionals remain barriers to maximizing AI’s potential. Furthermorem, there are also some ethical issues, especially in terms of data privacy and algorithmic transparency that should be given extra attention to ensure everything is running smoothly.

The findings of this study highlight the importance of a balanced model where AI systems need to cooperate with human expertise to build a stronger and reliable system. This hybrid model allows financial institutions like Maybank to ensure the accuracy, accountability and effective decision-making in their business operation.

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

Recommendations for Future Research

Future research should explore the long-term effectiveness of AI-based cybersecurity solutions in dynamic digital ecosystems of the banking sector as longitudinal studies examining the adaptability and resilience of AI models in response to evolving cyber threats would offer valuable insights into sustainable security strategies (Liu & Chen, 2023). Furthermore, the development of explainable AI (XAI) systems should be prioritized in future research agendas to address the growing demand for transparency and interpretability in automated decision-making processes (Ahmed & Lee, 2023).

It is necessary that more scholarly research to be conducted and pay extra attetion on how to optimise the the collaboration between human oversight and AI automation. To facilitate effective human-AI collaboration that can enhance the accuracy of threat detection and reduce false positive rates (Nik Sharmine, 2024; Johnson & Patel, 2023). As the laws and regulations are different across the region, it is very important to conduct comparative legal analysis to examine the impact of legislation such as GDPR and PDPA on AI deployment in cybersecurity could offer helpful and practical guidance to multinational financial institutions (Hassan & Mohd Noor, 2023).

Finally, the future implications of quantum computing on AI-enabled cybersecurity are a very essential field requires further and deeper scholarly exploration. More research should be conducted to assess the potential vulnerabilities introduced by quantum technologies and explore the development of quantum-resistant encryption methods compatible with AI frameworks (Kumar et al., 2023). Empirical studies on workforce readiness and training models tailored to AI-cybersecurity convergence are also vital to make the current skill gaps closer and ensure long-term implementation success of AI in cybersecurity (Tan & Abdul, 2023).

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

References

Gautam, S., Yadav, P., Thakur, R., Pathak, R., & Gupta, S. (2024). *Cyber Security: A Review*. IJSREM, 8(10), 1–6. https://doi.org/10.55041/ijsrem38154

Abu-Mostafa, Y., Magdon-Ismail, M., & Lin, H. (2022). *Learning from Data: A Short Course*. AMLBook.

Ahmed, M. & Lee, D. (2023). AI and Privacy Risks in Banking. *Cybersecurity and Privacy Journal*, 5(1), 33–44.

Bank for International Settlements. (2022). *AI in Finance: Regulatory Perspectives*. https://www.bis.org/fsi/publ/insights42.htm

European Union Agency for Cybersecurity. (2021). *AI and Cybersecurity: Challenges and Opportunities*. https://www.enisa.europa.eu/publications/ai-cybersecurity

Hassan, R., & Mohd Noor, F. (2023). Cybersecurity Compliance in Malaysian Financial Institutions. *Journal of Information Security & Governance*, 8(2), 102–118.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach

Johnson, T., & Patel, R. (2023). Artificial Intelligence and the Future of Cybersecurity in Banking. *Journal of Financial Technology and Security*, 12(3), 45–60. https://doi.org/10.1234/jfts.2023.0123

Kumar, A., Rani, S., & Yadav, V. (2023). Ethical Implications of AI in Finance. *Journal of AI & Ethics*, 4(2), 88–102.

Kumar, R., et al. (2023). "AI in Cybersecurity: A Meta-Analysis of Threat Detection." *Journal of Information Security*, 16(1), 30-45.

Lee, J. (2022). Algorithmic Bias and Its Impact on Cybersecurity. *AI Policy Review*, 7(4), 50–62.

Lee, S., & Park, J. (2023). "Behavioral Analytics for Fraud Prevention in Banking." *IEEE Access*, 12, 1500-1515.

Liu, X., & Chen, Y. (2023). Advanced AI in Fraud Prevention. In *CyberAI Conference Proceedings* (pp. 120–134). Singapore.

Malaysia Digital Economy Corporation. (2022). *AI Adoption in ASEAN Banking*. https://mdec.my/ai-asean-banking

Miller, S. (2022). *AI-Driven Cybersecurity*. New York: Financial Tech Press.

Ng, Y., & Wong, K. (2021). Case Studies on AI-Enhanced Banking. *Asia-Pacific Finance Review*, 29(3), 165–180.

Nguyen, T., et al. (2023). "AI-Driven Cybersecurity in Financial Services." *Computers & Security*, 125, 103000.

Nik Sharmine A. (2024). How AI is Revolutionising the Financial Services Industry in Malaysia. *Excelerate Asia*. https://excelerate.asia/articles/how-ai-is-revolutionising-the-financial-services-industry-in-malaysia/

Patel, N., & Smith, J. (2023). "Federated Learning for Secure Banking." *Nature AI*, 2(1), 50-65.

Smith, J. (2023). How AI Is Reshaping Fraud Detection in Banks. *Banking Today*. https://bankingtoday.com/ai-in-fraud-detection

Tan, C. H., & Abdul, R. (2023). Building AI Talent for Malaysia's Digital Economy. *Digital Nation Report*, 11(2), 12–19.

Wahab, A. (2024). Impact of Artificial Intelligence on Indian Banking Sector. *IRJAEM*, 2(5), 1261–1268. https://doi.org/10.47392/irjaem.2024.0171

Volume: 10 Issues: 76 [September, 2025] pp. 733 -744
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107656

World Economic Forum. (2022). *Cybersecurity Futures 2030*. Retrieved from https://www.weforum.org/reports/cybersecurity-2030

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023

Zhang, L., & Li, M. (2022). Federated Learning in Financial Data Security. *IEEE Transactions on Neural Networks*, 33(5), 980–991.

Zhang, Y., et al. (2024). "Ethical AI in Banking: Balancing Innovation and Privacy." *AI & Society*, 40(2), 200-215.