*International Journal of Scientific Research and Modern Technology (IJSRMT)* *ijsrmt.com*
*Volume 5, Issue 2, 2026*
*DOI: https://doi.org/10.38124/ijsrmt.v5i2.1246*

# Generative AI-Based Threat Model for Improving Cybersecurity in the Banking Sector

Muhamed Ramees Cheriya Mukkolakkal[1]

Publication Date: 2026/02/24

**Abstract**

In this systematic review paper, it discusses how generational artificial intelligence affects the banking sector and cybersecurity, identifies gaps in the current security systems, and highlights the importance of dynamic, AI-based threat mitigation structures. The findings recommend the development of predictive, smart, and resistant cybersecurity systems that can meet modern digital banking contexts.

***Keywords:*** *Generational AI; Threat Modelling; AI Governance; Cyber Risk; Adaptive Security Systems, Banking Cybersecurity; Digital Banking.*

## I. INTRODUCTION

➢ *Background*

In the banking industry, artificial intelligence is increasingly being used to improve customer experience, optimise operations, prevent fraud, and increase the effectiveness of risk management. However, the very technologies that bring about positive outcomes also create new and sophisticated cybersecurity threats (Alkhdour, AlWadiand Alrawad, 2024). GenAI can be used to design phishing emails with high levels of credibility, voice impersonation, malware robots, identity impersonation, and social engineering beyond what all other cyber-threats are capable of doing.

Banks work in an extremely controlled milieu and have access to sensitive financial and personal information, which makes them the most attractive victims of cybercriminals. Conventional security frameworks and threat models are mostly reactive and based on past attack patterns, which makes them mostly ineffective in the quickly changing and AI-driven threat environment (Mishra, 2023). As a result, the need to be proactive and adaptive threat models with specifications that are tailored to counter the threats presented by Generational AI is increasing in demand. An AI-based threat model in the banking industry can help organisations predict, assess, and reduce the emergent risks more efficiently.

➢ *Problem Statement*

The current threat models used in the banking sector in terms of cybersecurity are inadequate to identify, forecast, or discourage threats that are generated by sophisticated AI-based technologies. With the help of GenAI, which allows automating attacks and personalising phishing messages, as well as bypassing traditional detection systems, banks face an increased risk of fraud, data leakage, and losses (PATTANAYAK, 2023). Lack of a well-designed, AI-related threat-modelling system will limit the ability of banks to effectively handle these evolving risks.

➢ *Research Aim and Objectives*

The purpose of the research is to evaluate a generative AI-based threat model that focuses on improving cybersecurity in the banking sector.

- *Objectives:*

✓ To identify the major cyber security threats, it has been introduced by the generational AI in the banking sector.
✓ To examine the existing cybersecurity framework in banking and address its limitations for evaluating the AI-driven threats.
✓ To focus on developing strong generational AI-based threat models which focus on improving threat detection and mitigation in the banking security system.

➢ *Research Questions*

- What are the major cybersecurity threats that have been introduced by generative AI in the banking sector?
- What is the limitation that the existing banking cybersecurity framework have for addressing the generational-AI-based threat?

Mukkolakkal, M. R. C. (2026). Generative AI-Based Threat Model for Improving Cybersecurity in the Banking Sector. *International Journal of Scientific Research and Modern Technology*, *5*(2),34–44. https://doi.org/10.38124/ijsrmt.v5i2.1246

- How can a new threat model of generation AI-based focus on improving the detection and mitigation of Cyber threats in the banking system?

➢ *Research Rationale*

The study is critical since the abuse of Generational AI is a fast-growing threat that compromises the confidentiality, integrity, and safety of banking systems. By demystifying AI-based threats and developing proper threat models, the banks will strengthen their cyber resilience, reduce fraud, protect customer information, and comply with the regulations. The study has academic value by applying the threat-modelling literature to the field of GenAI and is practical in offering a framework which a bank can use to improve its security position.

## II. LITERATURE REVIEW

➢ *Understanding Generational AI and Its Security Implications*

With each new generation, computational capabilities and independence increase, and become more and more closely integrated into organisational functions, which in turn enhances the efficiency of operations and also increases their vulnerability to cyber risk (Kahila et al., 2023). The growing capacities of AI systems that increasingly enter financial services create new vulnerabilities that relate to the misuse of data, abuse of automation, manipulation of models, and obscurity (Chinnappappaiyan, 2025). The user interactions with AI technologies have a strong impact on security performance since a lack of user security behaviour and excessive use of automated systems make them more vulnerable to exploitation and social engineering (Castaneda, 2025). The articles that investigate the Generation Z generation highlight the issues that revolve around the ethical, privacy, and governance risks of advanced AI technologies, hence implying that social acceptance and trust are closely linked to the views of AI security and accountability (Gupta et al., 2024; Kacperska et al., 2024).

The expansion of AI to mobile, cloud, and high-performance computing infrastructures also brings forth the issues of compounded privacy, authentication, and infrastructure threats, especially in the high-speed digital ecosystems like banking systems (Gundu et al., 2022). In addition, the increasing agency of AIs diminishes human control, thereby weakening error detection, responsibility and regulation systems in areas of the economy that could impact security, like the financial sector (Kahila et al., 2023). These trends underscore the idea that generational AI not only alter modalities by which cyber threats are implemented but also changes the socio-technical context on which banking security is carried out, which in turn demands more adaptive and future-oriented approaches to the threat conceptualisations (Chinnappappiyan, 2025).

➢ *Cyber Security Threats Existing in the Banking Sector*

The banking industry remains one of the main targets of cybercrime because of the availability of high-value financial resources and critical information coupled with the level of digital interconnectivity (Mishra, 2023; Al-Dosari et al., 2024). Phishing, ransomware, identity theft, account takeover, insider, and payment fraud are the most common examples of threats; they continue to grow in number as banking systems are digitised and more reliant on clouds (Ghelani et al., 2022; Vinoth et al., 2022). The digital transformation initiatives only serve to increase these threats by creating bigger attack surfaces through mobile banking, APIs, fintech partnerships, and third-party service providers (Saeed et al., 2023b).According to systematic reviews, cyber threats affect consumer trust and utilisation of digital banking services significantly because the perceived risks of cybercrimes affect user behaviour and institutional credibility (Cele and Kwenda, 2025). There is also a growing regulatory pressure on financial organisations to be technologically resilient, and numerous organisations are unable to balance technological progress with the level of security measures (Alkhdour et al., 2024; Hassan et al., 2024). Although AI enhances the functionality of the defence, it is equally susceptible to attacks (poisoning), thereby making AI systems susceptible to evasion (Admass et al., 2024).

➢ *Challenges faced in the existing model*

Banking Traditional cybersecurity models in the past have been based largely on an intensive dependency on rule-based detection, historical threat databases, and on models of defence that are perimeter-based (Saeed et al., 2023a). Current models do not have the ability to dynamically learn new attack patterns, predict new risks, or dynamically change, which limits their usefulness in the modern threat space (Admass et al., 2024). The ethical, regulatory, and governance complexities in the implementation of advanced AI in security systems are another major problem.

Banks should comply with strict data protection regulations, transparency requirements, and audit issues, which may be incompatible with shadowy and self-directed AI models (Doddipatla, 2024; Botunac et al., 2024). This paradox of innovation and compliance often ends up limiting the adoption or leads to half-baked and ineffective implementations (Pamarthi, 2024; Mucsková, 2024). Also, the lack of user awareness, organisational preparedness, and cyber expertise undermines the effectiveness of the existing security models, with human factors being one of the most significant factors in cyber incidents (Castaneda, 2025; Gupta et al., 2024). Without a holistic theory of technical, organisational, and human aspects that consider each other simultaneously, the existing banking security models are not sufficient to control the risks posed by generational AI.

➢ *Theoretical Framework*

The study is based on the socio-technical systems theory, cyber risk management theory and adaptive security theory. The two views justify why technological, organisational and human variables interact to influence the result of cyber security in banks. Generational AI is tailored as an evolving technological force that changes behaviour of threat, vulnerability of the system and

exposure to risks. The framework facilitates the examination of the impacts of the developing AI capabilities on the effectiveness of security and the justification of having adaptable, intelligence-driven threat models to address the emergent cyber threats.

## III. MATERIALS AND METHODS

➢ *Search Strategy*

A search in literature was conducted within Scopus, IEEE Xplore, and Google Scholar, where the keywords were related to Generational AI, banking security, and cyber threats and narrowed to peer-reviewed studies in the English language.

Table 1 Inclusion and Exclusion Criteria for SLR

| Criteria | Inclusion | Exclusion |
|---|---|---|
| Source type | Peer-reviewed journals, conference papers | Blogs, news articles |
| Language | English | Non-English |
| Topic relevance | Generational AI and banking security | Unrelated AI or non-banking studies |
| Time period | 2019–2025 | Studies before 2019 |

(Source: Self-Created)

➢ *Study Selection Using PRISMA Framework*

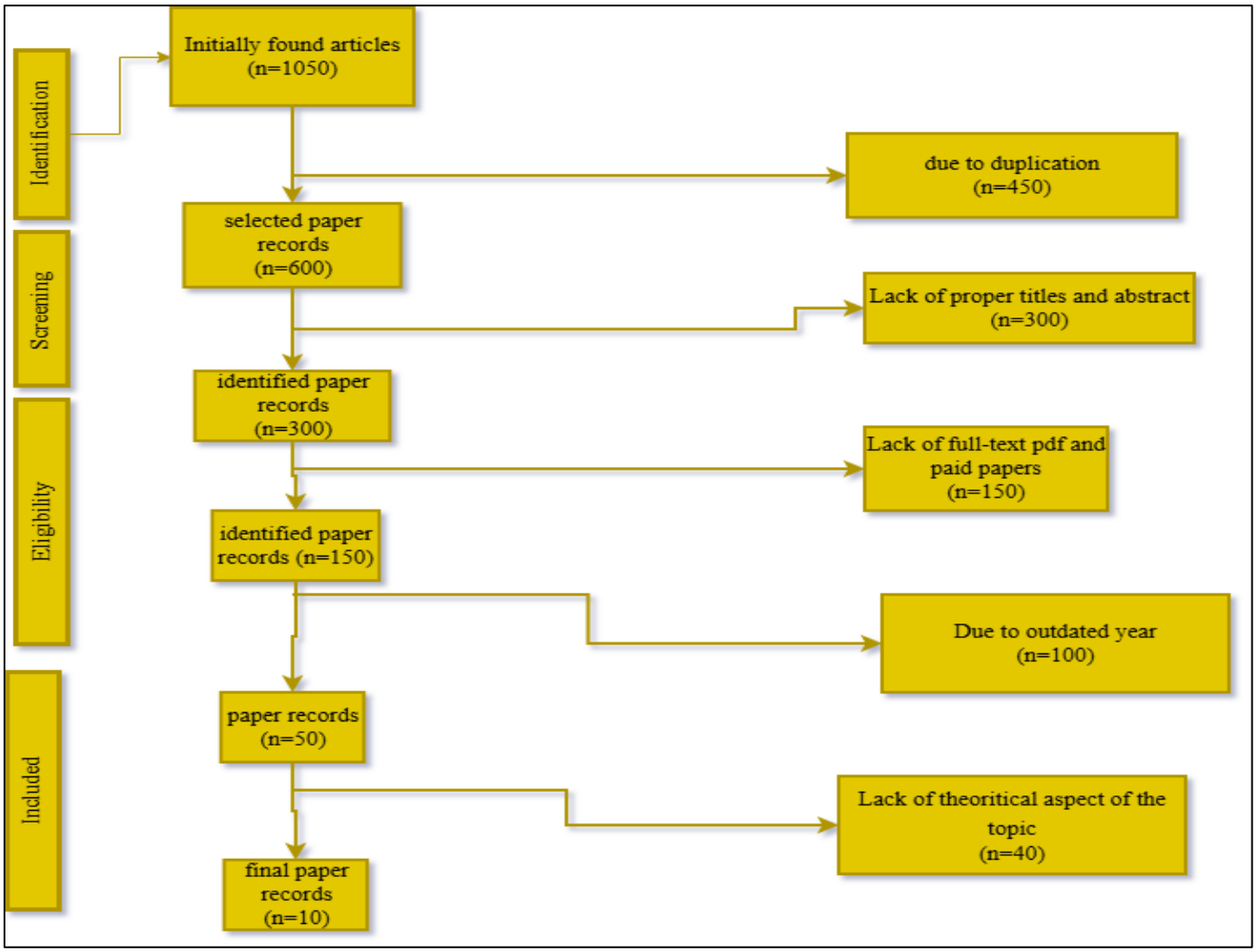


Fig 2 Prisma Diagram
(Source: Self-Created)

➢ *Data Analysis Technique*

Thematic analysis was used to determine, discuss, and present trends in the data gathered. Following the six-step model centres and methods by Braun and Clarke, the process included familiarisation with the data, initial code generation, theme searching, theme reviewing, theme definition and naming, and final report production. This methodology supported a highly strict, open, and systematic understanding of qualitative results on Generational AI threats and banking security.

## IV. RESULTS AND DISCUSSION

- *Theme 1: Evolution of Generational AI and Its Impact on Banking Security*

According to the current study, the development of artificial intelligence in generation after generation has essentially revolutionised the banking operations and security environments. Higher levels of AI technologies enable individual digital banking, identify fraud, and engage the customer via mobile platforms, which contribute to higher efficiency and ease of use of the systems (Manser Payne et al., 2021; Sultana and Faisal, 2024; Paramesha et al., 2024). The addition of AI to cloud-native and hybrid systems is an additional issue to the security management problem, since banking systems have now been dispersed into heterogeneous environments that require cohesive and clever security frameworks (Oladosu et al., 2022). There is a growing trend toward automated decision-making, which eliminates direct human control, which in turn complicates the possibility of early detection of mistakes, anomalies and ill intentions (Ngubane and Njenga, 2025). Such changes highlight the fact that generational AI can act as a security-facilitating mechanism and a risk-enhancing tool in modern banking (Paramesha et al., 2024).

- *Theme 2: Limitations of Existing Banking Cyber Security Models*

The findings indicate that the conventional banking cybersecurity models are largely reactive and more static as they are based on fixed, predefined rules and past attack history that are not adequate to overcome the dynamically emerging cyber threats. The dynamic nature of contemporary digital banking risks may be challenging to represent in risk assessment frameworks, especially risks brought about by AI-based automation and massive data processing (Saha et al., 2025; Shulha et al., 2022). This is a weakness of the current systems, as they can no longer effectively identify new or evolving attack behaviour patterns. Even though machine learning and biometric authentication can enhance the detection of fraud and help verify an identity, they are often used separately, without being integrated into a comprehensive and dynamic system of security (Asmar and Tuqan, 2024; Khan et al., 2023). Cyber threats are becoming more sophisticated, and this hurts customer confidence and digital banking adoption because customers have privacy concerns, fraud and data security (Waliullah et al., 2025). Although AI-based fraud detection improves the ability to detect anomalies, it is prone to poor data quality, a bias in the model and adversarial examples, making it untrustworthy as a single solution (Olowu et al., 2024; Sarker et al., 2020; Kumar and Kiran, 2025).

- *Theme 3: Need for an Adaptive Generational AI-Based Threat Model*

The results severely highlight the growing need of adaptive, generational AI-based threat models capable of predicting, simulating and responding to cyber threats in real-time. The pace, magnitude and acumen of AI-based attacks make traditional, unchanging models insufficient hence the need to embrace proactive defence mechanisms (Buehler et al., 2024). Threat intelligence systems that are built using AI and are based on behavioural analytics, predictive modelling, and simulating attacks enhance cybersecurity by also enhancing situational awareness and improving prompt and evidence-driven reactions (Rauf et al., 2025; Chaganti 2024; Zacharis et al., 2024). An evasion based AI threat modelling is a continuously evolving system behaviour and new attack patterns, thus it only anticipates the possible threats instead of just detecting them after they have occurred. This reactive-preventative shift in security has been a paradigm shift in the approach to cybersecurity (Yaseen, 2023). Next-generation security systems combine AI-based monitoring, prediction, and automatic response systems into cloud and network worlds, thus providing constant adaptation to new and unidentified threats (Akbar and Zafer, 2024; Sivakumar et al., 2025). Also, national-level cybersecurity models emphasise the significance of intelligence-based, coordinated defence measures to deal with the large-scale cross-sector cyber threat (Siam et al., 2025). An adaptive generational AI-based threat model enables continuous identification, analysis, and anticipation of cyber threats through real-time learning and simulation. By dynamically adjusting to new attack patterns and threat behaviours, such models shift security from reactive detection to proactive prevention, ensuring resilient and future-oriented cybersecurity protection. Taken together, these observations shed light on the fact that adaptive generational AI-based models of threat are essential to the development of robust, future-oriented cybersecurity systems in the sophisticated digital landscape.

- *Discussion*

The findings show that, as generational AI considerably improves the efficiency and security capabilities of the banking industry, it also creates complex and dynamic risks that are beyond the scope of conventional security models (Sachan, Lakhani and Poddar, 2025). The drawbacks of fixed structures, compartmentalisation of AI implementation, and the ability to implement governance methods show the need to develop a single, adaptive, and intelligence-based threat model to the banking context (Coombs, 2024). A balanced approach to resilient, transparent, and trustworthy banking security systems may be provided by an adaptive generational AI-based threat model that combines predictive analytics, continuous learning, regulatory compliance, and oversight by humans.

## V. CONCLUSION AND RECOMMENDATIONS

- *Summary of Key Findings*

The current research paper has explored how generational artificial intelligence affects banking cybersecurity, the constraints of the current security models, and the necessity of adaptive threat models. The analysis also found that generational AI has significantly improved the efficiency of banking, automation, and fraud

detection, but also raised the complexity of systems, attack surfaces, and vulnerability exposure. The digital banking solutions that are run with the help of AI are based on interconnected systems and cloud infrastructure and automated decision-making, which can increase the risk of cyber-attacks, data breaches and system manipulations. The research has also established that the conventional banking cybersecurity models are so stagnant, reactive, and reliant on past threat information that they cannot be used to address developed and AI-based cybersecurity threats.

- *Linking Findings with Objectives*

The first objective was to define and discuss generational AI-based threats in banking; the former goal was accomplished through the demonstration of increasing automation, connectivity, and system dependence of AI evolution, which results in increased risks of fraud, identity theft, and data manipulation. The second aim was to review the weaknesses of the current banking cybersecurity frameworks; the results proved that the current models are not adaptive enough, reactive and rule-based, which makes them unable to deal with dynamic and intelligent cyber threats. The third goal was to recommend the necessity of generational AI-based threat models; the findings of the work are highly constructive towards this goal as they demonstrated the advantages of predictive, adaptive and intelligence-selection security models, which can answer changing threats in real-time.

- *Recommendations*

The use of adaptive, AI-powered threat models that incorporate predictive analytics, behavioural monitoring, and automated response mechanisms into the security infrastructure is advised to be implemented by banks (Terziyan et al., 2025). Financial institutions are advised to invest in integrated security architectures to integrate fraud detection systems and identity management systems, cloud security systems and threat intelligence systems into a single system (Radanliev, Santos and Ani, 2025). Governance should also be highly valued in AI security systems by banks, with transparency and explainability of these systems, so that regulatory requirements are adhered to and that customers' trust is maintained. To deal with human vulnerabilities, regular staff training and cyber awareness programmes are to be introduced. Lastly, it is important to continuously evaluate and update threat models to have resiliency to future AI-based cyber threats.

## REFERENCES


[1]. Adejumo, A. and Ogburie, C., (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), pp.1527-1541.https://www.researchgate.net/profile/Adetunji-Adejumo/publication/390166305_Strengthening_finance_with_cybersecurity_Ensuring_safer_digital_transactions/links/67e2c626fe0f5a760f90195d/Strengthening-finance-with-cybersecurity-Ensuring-safer-digital-transactions.pdf

[2]. Admass, W.S., Munaye, Y.Y. and Diro, A.A., (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, p.100031. https://www.sciencedirect.com/science/article/pii/S2772918423000188

[3]. Akbar, R. and Zafer, A., (2024). Next-Gen Information Security: AI-Driven Solutions for Real-Time Cyber Threat Detection in Cloud and Network Environments. *J. Cybersecur. Res*, *12*, pp.123-145.https://www.researchgate.net/profile/Ali-Zafer-3/publication/385417618_Next-Gen_Information_Security_AI-Driven_Solutions_for_Real-Time_Cyber_Threat_Detection_in_Cloud_and_Network_Environments/links/6723b68277f274616d541f34/Next-Gen-Information-Security-AI-Driven-Solutions-for-Real-Time-Cyber-Threat-Detection-in-Cloud-and-Network-Environments.pdf

[4]. AL-Dosari, K., Fetais, N. and Kucukvar, M., (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, *55*(2), pp.302-330. https://www.tandfonline.com/doi/pdf/10.1080/01969722.2022.2112539

[5]. Alkhdour, T., AlWadi, B.M. and Alrawad, M., (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, *14*(3), pp.167-190. https://jisis.org/wp-content/uploads/2024/09/2024.I3.010.pdf

[6]. Asmar, M. and Tuqan, A., (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon*, *10*(17).https://www.cell.com/heliyon/pdf/S2405-8440(24)13602-X.pdf

[7]. Botunac, I., Parlov, N. and Bosna, J., (2024, June). Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA. In *2024 13th Mediterranean Conference on Embedded Computing (MECO)* (pp. 1-6). IEEE. https://www.researchgate.net/profile/Ive-Botunac/publication/381963649_Opportunities_of_Gen_AI_in_the_Banking_Industry_with_regards_to_the_AI_Act_GDPR_Data_Act_and_DORA/links/668655a3714e0b031543a7ca/Opportunities-of-Gen-AI-in-the-Banking-Industry-with-regards-to-the-AI-Act-GDPR-Data-Act-and-DORA.pdf

[8]. Buehler, K., Corsi, A., Weintraub, B., Jurisic, M., Siani, A. and Lerner, L. (2024). *Scaling gen AI in banking: Choosing the best operating model*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/scaling-gen-ai-in-banking-choosing-the-best-operating-model

[9]. Castaneda, N., (2025). Analysis of user security practices in Gen AI. https://www.theseus.fi/bitstream/handle/10024/890396/Castaneda_Noah.pdf?sequence=2

[10]. Cele, N.N. and Kwenda, S., (2025). Do cybersecurity threats and risks have an impact on

the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), pp.31-48.https://www.emerald.com/insight/content/doi/10.1108/jfc-10-2023-0263/full/pdf

[11]. Chaganti, K.C., (2024). Leveraging Generative AI for Proactive Threat Intelligence: Opportunities and Risks. *Authorea Preprints*.https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.173388012.23004648

[12]. Chinnappaiyan, B., (2025). Navigating AI Security Challenges Across Industries: Best Practices for Secure Adoption of Generative and Agentic AI Systems. *Journal of Computer Science and Technology Studies*, *7*(6), pp.294-300. https://al-kindipublishers.org/index.php/jcsts/article/download/9966/8660

[13]. Coombs, M.R.A., (2024). AI Integration for Scenario Development. *Military Review*, *1*.https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2024/AI-Integration/AI-Integration-for-Scenarios-UA1.pdf

[14]. Darem, A.A., Alhashmi, A.A., Alkhaldi, T.M., Alashjaee, A.M., Alanazi, S.M. and Ebad, S.A., (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEe Access*, *11*, pp.125138-125158. https://ieeexplore.ieee.org/iel7/6287639/6514899/10292652.pdf

[15]. Doddipatla, L., (2024). Ethical and Regulatory Challenges of Using Generative AI in Banking: Balancing Innovation and Compliance. *Educational Administration: Theory and Practice*, *30*(3), pp.2848-2855. https://www.academia.edu/download/120582512/ap_2075_vol._30_no._32024_educational_administration_theory_and_practice_1_alpha_publication.pdf

[16]. Ghelani, D., Hua, T.K. and Koduru, S.K.R., (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea Preprints*. https://www.authorea.com/doi/pdf/10.22541/au.166385206.63311335

[17]. Gundu, S.R., Charanarur, P., Chandelkar, K.K., Samanta, D., Poonia, R.C. and Chakraborty, P., (2022). Sixth-Generation (6G) Mobile Cloud Security and Privacy Risks for AI System Using High-Performance Computing Implementation. *Wireless Communications and Mobile Computing*, *2022*(1), p.4397610. https://onlinelibrary.wiley.com/doi/pdf/10.1155/2022/4397610

[18]. Gupta, A., Pranathy, R.S., Binny, M., Chellasamy, A., Nagarathinam, A., Pachiyappan, S. and Bhagat, S., (2024). Voices of the future: Generation Z's views on AI's ethical and social impact. In *Technology-Driven Business Innovation: Unleashing the Digital Advantage, Volume 1* (pp. 367-386). Cham: Springer Nature Switzerland. https://www.researchgate.net/profile/Sathish-Pachiyappan-3/publication/379234845_Voices_of_the_Future_Generation_Z%27s_Views_on_AI%27s_Ethical_and_Social_Impact/links/66c6bbf697265406eaa07771/Voices-of-the-Future-Generation-Zs-Views-on-AIs-Ethical-and-Social-Impact.pdf#page=366

[19]. Hassan, A.O., Ewuga, S.K., Abdul, A.A., Abrahams, T.O., Oladeinde, M. and Dawodu, S.O., (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), pp.41-59. https://www.researchgate.net/profile/Temitayo-Abrahams-2/publication/379038844_CYBERSECURITY_IN_BANKING_A_GLOBAL_PERSPECTIVE_WITH_A_FOCUS_ON_NIGERIAN_PRACTICES/links/65f80f52c05fd268801fc583/CYBERSECURITY-IN-BANKING-A-GLOBAL-PERSPECTIVE-WITH-A-FOCUS-ON-NIGERIAN-PRACTICES.pdf

[20]. Kacperska, E.M., Stefańczyk, J., Dąbrowski, P.J. and Załoga, W., (2024). The Consequences of Implementing Artificial Intelligence Technology in the Digital Economy from the Perspective of Generation Z. *European Research Studies Journal*, *27*(3), pp.1039-1057. https://ersj.eu/journal/3764/download/The+Consequences+of+Implementing+Artificial+Intelligence+Technology+in+the+Digital+Economy+from+the+Perspective+of+Generation+Z.pdf

[21]. Kahila, J., Jormanainen, I., Pope, N., Vartiainen, H. and Tedre, M., (2023, March). Generation ai: Ai education for the security mindset (genai). In *Society for Information Technology & Teacher Education International Conference* (pp. 28-31). Association for the Advancement of Computing in Education (AACE). https://www.researchgate.net/profile/Juho-Kahila/publication/385531303_Generation_AI_AI_Education_for_the_Security_Mindset_GenAI/links/6729b9d22326b47637c7cc42/Generation-AI-AI-Education-for-the-Security-Mindset-GenAI.pdf

[22]. Khan, H.U., Malik, M.Z., Nazir, S. and Khan, F., (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. *Ieee Access*, *11*, pp.80181-80198.https://ieeexplore.ieee.org/iel7/6287639/6514899/10194299.pdf

[23]. Kumar, R. and Kiran, S., (2025). AI-Driven Frameworks for Unsupervised Fraud Detection in Banking Cybersecurity. *Int. J. Sci. Eng. Appl*, *14*(3), pp.1-5.https://ijsea.com/archive/volume14/issue3/IJSEA14031006.pdf

[24]. Manser Payne, E.H., Peltier, J. and Barger, V.A., (2021). Enhancing the value co-creation process: artificial intelligence and mobile banking service platforms. *Journal of Research in Interactive Marketing*, *15*(1), pp.68-85.https://www.researchgate.net/profile/Liz-Manser-Payne/publication/349282586_Enhancing_the_value_co-creation_process_artificial_intelligence_and_mobil

e_banking_service_platforms/links/609719b5458515d31507d5bb/Enhancing-the-value-co-creation-process-artificial-intelligence-and-mobile-banking-service-platforms.pdf

[25]. Mishra, S., (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, *13*(10), p.5875. https://www.mdpi.com/2076-3417/13/10/5875

[26]. Mohammed, A., (2025). Blockchain-Driven Cybersecurity Audits: Securing Financial Systems with Trust and Transparency. *Authorea Preprints*. https://www.authorea.com/doi/pdf/10.22541/au.173862082.22380043

[27]. Mucsková, M., (2024). Transforming banking with artificial intelligence: Applications, challenges, and implications. *Trends Economics and Management*, *18*(42), pp.21-37. https://journals.vutbr.cz/index.php/trends/article/download/609/588

[28]. Ngubane, N. and Njenga, K., (2025). A complex conundrum of Information security in virtual banking. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *7*(5), pp.397-410.https://bussecon.com/ojs/index.php/ijbes/article/download/974/587

[29]. Oladosu, S.A., Ige, A.B., Ike, C.C., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., (2022). Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. *International Journal of Science and Technology Research Archive*, *3*(2), pp.270-280.https://www.researchgate.net/profile/Olukunle-Amoo/publication/387005022_Next-generation_network_security_conceptualizing_a_Unified_AI-Powered_Security_Architecture_for_Cloud-Native_and_On-Premise_Environments/links/67798e8fe74ca64e1f4babf7/Next-generation-network-security-conceptualizing-a-Unified-AI-Powered-Security-Architecture-for-Cloud-Native-and-On-Premise-Environments.pdf

[30]. Olowu, O., Adeleye, A.O., Omokanye, A.O., Ajayi, A.M., Adepoju, A.O., Omole, O.M. and Chianumba, E.C., (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *Advanced Research and Review*, *21*(2), pp.227-237.https://www.researchgate.net/profile/Ernest-Chianumba/publication/386276951_AI-driven_fraud_detection_in_banking_A_systematic_review_of_data_science_approaches_to_enhancing_cybersecurity/links/67863f622be36743a5d571d6/AI-driven-fraud-detection-in-banking-A-systematic-review-of-data-science-approaches-to-enhancing-cybersecurity.pdf

[31]. Pamarthi, K., (2024). Analysis On Opportunities And Challenges Of Ai InThe Banking Industry. *Journal ID*, *1232*, p.1214. https://www.researchgate.net/profile/Kartheek-Pamarthi/publication/389754095_Analysis_on_Opportunities_and_Challenges_of_AI_in_the_Banking_Industry/links/67d12fa8bab3d32d8440f6a4/Analysis-on-Opportunities-and-Challenges-of-AI-in-the-Banking-Industry.pdf

[32]. Paramesha, M., Rane, N. and Rane, J., (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review. *Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review (June 6, 2024)*.https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4855893

[33]. PATTANAYAK, S.K., (2023). Generative AI and Its Role in Shaping the Future of Risk Management in the Banking Industry. https://www.researchgate.net/profile/Suprit-Kumar-Pattanayak/publication/387470906_Generative_AI_and_Its_Role_in_Shaping_the_Future_of_Risk_Management_in_the_Banking_Industry/links/676f2b4afb9aff6eaaf292d5/Generative-AI-and-Its-Role-in-Shaping-the-Future-of-Risk-Management-in-the-Banking-Industry.pdf

[34]. Puchakayala, P.R.A., (2024). Generative Artificial Intelligence Applications in Banking and Finance Sector. *Master's thesis, University of California, Berkeley, CA, USA*. https://www.researchgate.net/profile/Praneeth-Reddy-Amudala-Puchakayala/publication/387519004_Generative_Artificial_intelligence_Applications_in_Banking_and_Finance_sector/links/67f5483649e91c0feaea0470/Generative-Artificial-intelligence-Applications-in-Banking-and-Finance-sector.pdf

[35]. Radanliev, P., Santos, O. and Ani, U.D., (2025). Generative AI cybersecurity and resilience. *Frontiers in Artificial Intelligence*, *8*, p.1568360.https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1568360/pdf

[36]. Rauf, H., Shah, S.I.H., Ali, T., Gul, H. and Soomro, M., (2025). USING GENERATIVE AI FOR SIMULATING CYBER SECURITY ATTACKS AND DEFENSE MECHANISMS: A NEW APPROACH TO AI-DRIVEN CYBER THREAT MODELING. *Spectrum of Engineering Sciences*, *3*(3), pp.361-381.https://www.sesjournal.com/index.php/1/article/download/218/204

[37]. Sachan, R.C., Lakhani, R. and Poddar, S., (2025). AI-enabled security mechanisms for WLANs: ensuring robust and adaptive protection in wireless networks. *World J. Adv. Res. Rev*, *25*(3), pp.2085-2095.https://www.researchgate.net/profile/Ram-Chandra-Sachan/publication/390368506_AI-enabled_security_mechanisms_for_WLANs_ensuring_robust_and_adaptive_protection_in_wireless_networks/links/67ef2464e8041142a162bc36/AI-enabled-security-mechanisms-for-WLANs-ensuring-robust-and-adaptive-protection-in-wireless-networks.pdf

[38]. Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A., (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), p.6666. https://www.mdpi.com/1424-8220/23/15/6666/pdf

[39]. Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. and Almuhaideb, A.M., (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), p.7273. https://www.mdpi.com/1424-8220/23/16/7273

[40]. Saha, S., Siddiki, M.S., Mondal, R.S., Bhuiyan, M.N.A. and Kamruzzaman, M., (2025). Risk assessment of cyber security in the banking sector. *Journal of Business and Management Studies*, *7*(4), pp.208-218.https://al-kindipublishers.org/index.php/jbms/article/download/10425/9140

[41]. Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A., (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), p.41.https://link.springer.com/content/pdf/10.1186/s40537-020-00318-5.pdf

[42]. Shulha, O., Yanenkova, I., Kuzub, M., Muda, I. and Nazarenko, V., (2022). Banking information resource cybersecurity system modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), p.80.https://www.mdpi.com/2199-8531/8/2/80/pdf

[43]. Siam, M.A., Shan-A-Alahi, A., Tuhin, M.K., Hossain, E., Bashir, M., Lucky, K.Y., Uddin, S.M.M. and Al Zaiem, A., (2025). AI-Driven Cyber Threat Intelligence Systems: A National Framework for Proactive Defense Against Evolving Digital Warfare. *Int. J. Comput. Exp. Sci. Eng*, *11*(3).https://www.researchgate.net/profile/Ahmed-Shan-A-Alahi/publication/395026968_AI-Driven_Cyber_Threat_Intelligence_Systems_A_National_Framework_for_Proactive_Defense_Against_Evolving_Digital_Warfare/links/68b18a3a3391fb1a7a4c270a/AI-Driven-Cyber-Threat-Intelligence-Systems-A-National-Framework-for-Proactive-Defense-Against-Evolving-Digital-Warfare.pdf

[44]. Sivakumar, J., Salman, N.R., Salman, F.R., Salimova, H.R. and Ghimire, E., (2025). AI-driven cyber threat detection: enhancing security through intelligent engineering systems. *Journal of Information Systems Engineering and Management*, *10*(19), pp.790-798.https://strathprints.strath.ac.uk/94351/1/Sivakumar-etal-JISEM-2025-AI-driven-cyber-threat-detection.pdf

[45]. Sultana, R. and Faisal, N.A., (2024). The Role Of Digital Banking Features In Bank Selection An Analysis Of Customer Preferences For Online And Mobile Banking. *Available at SSRN 5049165*.https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5049165

[46]. Terziyan, V., Tiihonen, T., Shukla, A.K., Gryshko, S., Golovianko, M., Terziyan, O. and Vitko, O., (2025). Towards ethical evolution: responsible autonomy of artificial intelligence across generations. *AI and Ethics*, pp.1-26.https://link.springer.com/content/pdf/10.1007/s43681-025-00759-9.pdf

[47]. Vinoth, S., Vemula, H.L., Haralayya, B., Mamgain, P., Hasan, M.F. and Naved, M., (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, pp.2172-2175. https://www.researchgate.net/profile/Mohd-Naved/publication/356761386_Application_of_cloud_computing_in_banking_and_e-commerce_and_related_security_threats/links/625cf5ae4173a21a0d1aaa9c/Application-of-cloud-computing-in-banking-and-e-commerce-and-related-security-threats.pdf

[48]. Waliullah, M., George, M.Z.H., Hasan, M.T., Alam, M.K., Munira, M.S.K. and Siddiqui, N.A., (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *arXiv preprint arXiv:2503.22710*.https://arxiv.org/pdf/2503.22710

[49]. Yaseen, A., (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, *7*(12), pp.25-43.https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf

[50]. Zacharis, A., Katos, V. and Patsakis, C., (2024). Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. *International Journal of Information Security*, *23*(4), pp.2691-2710.https://link.springer.com/content/pdf/10.1007/s10207-024-00860-w.pdf

[51]. Cheriya Mukkolakkal, M.R., (2025). InfraLLM: A Generic Large Language Model Framework for Production-Grade Microservice Auto-Scaling in Cloud Infrastructure. *International Journal of Scientific Research and Modern Technology*, *4*(11), pp.113-123. https://doi.org/10.38124/ijsrmt.v4i11.1023

[52]. Cheriya Mukkolakkal, M.R., (2024). IntelliStore: An Intelligent AI Agent Framework for Autonomous Storage and Database Optimization in Cloud-Native Microservices. *International Journal of Scientific Research and Modern Technology*, *3*(12), pp.243-250. https://doi.org/10.38124/ijsrmt.v3i12.1024

[53]. Mukkolakkal, M.R.C., (2025). Automated Detection of Network Card Bottlenecks in Apache Pulsar: An Enhanced Framework with Dynamic

Thresholds and Root Cause Analysis. *International Journal of Scientific Research and Modern Technology*, *4*(1), pp.228-232. https://doi.org/10.38124/ijsrmt.v4i1.1158

[54]. Mukkolakkal, M.R.C., (2025). Gen AI For ELT (Extract, Load, Transfer) in Streaming Application with Databricks/Snow Flakes. *International Journal of Scientific Research and Modern Technology*, *4*(12), pp.150-161. https://doi.org/10.38124/ijsrmt.v4i12.1209

[55]. Mukkolakkal, M.R.C., (2026). HierarchicalCDN: Federated Edge Intelligence with Metadata-Driven Cache Optimization for Live Streaming. *International Journal of Scientific Research and Modern Technology*, *5*(1), pp.140-145. https://doi.org/10.38124/ijsrmt.v5i1.1235

## Appendices

### Appendix 1: Summary Table

Table 2 Summary Table

| Authors | Theme | Key Findings | Methodology | Implications |
|---|---|---|---|---|
| Adejumo &Ogburie (2025) | Cybersecurity resilience | Cybersecurity improves financial trust | Conceptual review | Need stronger cyber frameworks |
| Admass et al. (2024) | Cyber challenges | Emerging cyber risks are increasing | Literature review | Continuous model updating |
| Akbar & Zafer (2024) | AI security | AI enables real-time threat detection | Conceptual model | Adopt AI-driven monitoring |
| AL-Dosari et al. (2024) | Banking AI | AI improves defence but adds complexity | Qualitative study | Balance innovation and risk |
| Alkhdour et al. (2024) | Banking risks | Cyber risks rising with digitalisation | Risk assessment | Enhance risk governance |
| Asmar &Tuqan (2024) | ML security | ML improves fraud detection | Empirical analysis | Integrate ML holistically |
| Botunac et al. (2024) | Regulation | Compliance shapes AI adoption | Policy analysis | Align AI with regulation |
| Buehler et al. (2024) | GenAI scaling | Organisational readiness is critical | Industry report | Structure AI operations |
| Castaneda (2025) | User behaviour | Human error drives vulnerabilities | Survey study | Improve user training |
| Cele & Kwenda (2025) | Trust & adoption | Cyber risk affects digital banking trust | Systematic review | Strengthen consumer security |
| Chaganti (2024) | Threat intelligence | AI enables proactive defence | Conceptual paper | Invest in AI threat modelling |
| Chinnappaiyan (2025) | AI security | Agentic AI introduces new risks | Best-practice review | Secure AI deployment |
| Coombs (2024) | Scenario modelling | AI improves security simulations | Conceptual analysis | Use AI in planning |
| Darem et al. (2023) | Threat classification | Banking threats are diversifying | Systematic review | Expand threat taxonomies |
| Doddipatla (2024) | Ethics | AI conflicts with compliance norms | Policy review | Strengthen AI governance |
| Ghelani et al. (2022) | Banking threats | Phishing and fraud dominate | Review study | Improve detection systems |
| Gundu et al. (2022) | Infrastructure risk | Cloud and 6G increase vulnerabilities | Technical analysis | Secure digital infrastructure |
| Gupta et al. (2024) | Ethics perception | Gen Z worries about AI misuse | Survey research | Address social trust |
| Hassan et al. (2024) | Regional practices | Cyber maturity varies by region | Comparative study | Localise security strategies |
| Kahila et al. (2023) | AI education | Security mindset is critical | Educational framework | Improve cyber awareness |
| Kacperska et al. (2024) | Economic impact | AI reshapes digital economy | Quantitative analysis | Support responsible AI |
| Khan et al. (2023) | Biometrics | Biometrics strengthen authentication | Systematic review | Deploy identity verification |

| | | | | |
|---|---|---|---|---|
| Kumar & Kiran (2025) | Fraud detection | AI improves anomaly detection | Framework proposal | Adopt unsupervised models |
| Manser Payne et al. (2021) | Mobile banking | AI enhances service value | Empirical study | Improve digital UX |
| Mishra (2023) | Financial AI | AI improves fraud monitoring | Empirical analysis | Expand AI in security |
| Mohammed (2025) | Blockchain security | Blockchain enhances auditability | Conceptual review | Combine blockchain + AI |
| Mucsková (2024) | AI transformation | AI improves banking efficiency | Review study | Manage transition risks |
| Ngubane & Njenga (2025) | Virtual banking | Virtual banking increases cyber exposure | Case analysis | Strengthen virtual controls |
| Oladosu et al. (2022) | Network security | Unified AI security improves protection | Architecture proposal | Deploy unified security |
| Olowu et al. (2024) | Fraud analytics | Data science enhances fraud detection | Systematic review | Improve data quality |
| Pamarthi (2024) | AI opportunities | AI improves competitiveness | Analytical review | Strategic AI investment |
| Paramesha et al. (2024) | AI applications | AI automates banking services | Comprehensive review | Align tech with governance |
| Pattanayak (2023) | Risk management | GenAI reshapes financial risk | Conceptual study | Update risk frameworks |
| Puchakayala (2024) | AI use cases | GenAI supports banking automation | Case-based analysis | Guide AI deployment |
| Radanliev et al. (2025) | Resilience | GenAI improves cyber resilience | Conceptual framework | Invest in resilience models |
| Rauf et al. (2025) | Attack simulation | AI simulates cyberattacks effectively | Experimental study | Use AI for testing |
| Saeed et al. (2023a) | Digital resilience | Cyber maturity enables resilience | Review study | Build cyber capabilities |
| Saeed et al. (2023b) | Threat intelligence | Intelligence improves preparedness | Systematic review | Adopt CTI systems |
| Saha et al. (2025) | Risk assessment | Existing models are static | Quantitative study | Move toward dynamic models |
| Sarker et al. (2020) | Cyber data science | ML supports cybersecurity analytics | Review study | Use data-driven defence |
| Shulha et al. (2022) | System modelling | Models fail to capture dynamics | Simulation study | Enhance model adaptability |
| Siam et al. (2025) | National defence | AI enables national cyber resilience | Framework proposal | Coordinate cyber defence |
| Sivakumar et al. (2025) | Intelligent security | Engineering AI improves detection | Empirical study | Integrate AI engineering |
| Sultana & Faisal (2024) | Customer behaviour | Digital features influence adoption | Survey study | Improve digital trust |
| Terziyan et al. (2025) | Ethical AI | Responsible AI is essential | Theoretical analysis | Implement ethical AI |
| Vinoth et al. (2022) | Cloud risk | Cloud banking increases exposure | Technical review | Strengthen cloud security |
| Waliullah et al. (2025) | Adoption risks | Cyber risk slows digital adoption | Systematic review | Reduce perceived risks |
| Yaseen (2023) | AI defence | AI shifts cybersecurity paradigms | Conceptual review | Transition to AI defence |
| Zacharis et al. (2024) | Forecasting | AI predicts cyber threat trends | Experimental design | Enable proactive security |

## Appendix 2: Thematic Table

Theme 1 Evolution of Generational AI and Its Impact on Banking Security

| Author(s) & Year | Focus Area | Key Findings | Relevance to Theme |
|---|---|---|---|
| Manser Payne et al. (2021) | AI in mobile banking | AI enhances customer engagement and service efficiency | Shows positive impact of AI evolution |
| Sultana & Faisal (2024) | Digital banking features | Digital features influence customer adoption | Demonstrates AI-driven transformation |
| Paramesha et al. (2024) | AI technologies in banking | AI, ML and blockchain reshape banking operations | Explains generational tech evolution |
| Ngubane & Njenga (2025) | Virtual banking security | Virtual banking increases security complexity | Shows new risks from AI-driven platforms |
| Oladosu et al. (2022) | AI-powered security architecture | Unified AI security is needed for hybrid systems | Highlights infrastructural impact of AI |

Theme 2 Limitations of Existing Banking Cyber Security Models

| Author(s) & Year | Focus Area | Key Findings | Relevance to Theme |
|---|---|---|---|
| Saha et al. (2025) | Cyber risk assessment | Traditional models are static and limited | Shows framework limitations |
| Shulha et al. (2022) | Cyber system modelling | Models fail to represent dynamic threats | Supports need for adaptability |
| Asmar &Tuqan (2024) | ML in cybersecurity | ML improves detection but lacks integration | Shows fragmentation issue |
| Khan et al. (2023) | Biometric systems | Biometrics strengthen authentication | Shows partial, isolated solutions |
| Waliullah et al. (2025) | Cyber risk and adoption | Cyber risks reduce digital banking adoption | Shows impact of ineffective models |
| Olowu et al. (2024) | AI fraud detection | AI systems vulnerable to data bias and manipulation | Highlights technical weaknesses |
| Sarker et al. (2020) | Cyber data science | ML depends heavily on data quality | Shows reliability limitations |
| Kumar & Kiran (2025) | Unsupervised fraud detection | AI detects anomalies but needs oversight | Shows AI not sufficient alone |

Theme 3 Need for an Adaptive Generational AI-Based Threat Model

| Author(s) & Year | Focus Area | Key Findings | Relevance to Theme |
|---|---|---|---|
| Rauf et al. (2025) | AI attack simulation | AI can simulate cyberattacks and defences | Supports proactive threat modelling |
| Chaganti (2024) | AI threat intelligence | AI enables proactive threat detection | Justifies adaptive models |
| Zacharis et al. (2024) | Threat forecasting | AI improves cyber threat prediction | Supports predictive defence |
| Akbar & Zafer (2024) | AI-driven detection | AI enables real-time threat monitoring | Supports real-time adaptability |
| Yaseen (2023) | AI threat response | AI shifts cybersecurity from reactive to proactive | Conceptual support for adaptive models |
| Sivakumar et al. (2025) | Intelligent engineering | AI enhances security engineering systems | Shows operational feasibility |
| Siam et al. (2025) | National cyber frameworks | Coordinated AI defence improves resilience | Shows strategic importance |