 ISSN:2302-8149
e-ISSN:2540-9719

The Role of Large Language Models in Enhancing Cybersecurity Measures: Empirical Evidence from Regional Banking Institutions

[1]Hewa Majeed Zangana*, [2]Harman Salih Mohammed, [3]Mamo Muhamad Husain
[1]Duhok Polytechnic University, Duhok, Iraq
[2]Ararat Technical Private Institute, Kurdistan Region - Iraq
[3]IT Dept., Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq
*e-mail: hewa.zangana@dpu.edu.krd

(***received*:** 9 March 2025, ***revised*:** 9 June 2025, ***accepted*:** 10 June 2025)

Abstract

The rapid advancements in artificial intelligence (AI) and machine learning (ML) have significantly influenced the cybersecurity landscape, particularly in the banking sector, where threats are increasingly sophisticated. Large Language Models (LLMs) such as OpenAI's GPT-4 and Google's BERT, offer novel approaches to threat detection, fraud prevention, and automated risk assessment. This paper explores the integration of Large Language Models (LLMs) in cybersecurity frameworks within financial institutions, highlighting their role in real-time anomaly detection, predictive analytics, and intelligent automation of security operations. By leveraging LLMs, banks can enhance their cybersecurity resilience, mitigate cyber threats, and improve regulatory compliance. However, challenges such as data privacy concerns, adversarial attacks, and computational resource demands must be addressed to ensure the secure and ethical deployment of these models. This study provides insights into the current applications, benefits, and limitations of Large Language Models (LLMs) in strengthening cybersecurity measures in the banking sector.

Keywords: artificial intelligence, banking cybersecurity, fraud detection, large language models, threat intelligence.

1 Introduction

The banking sector has witnessed a profound digital transformation, resulting in increased efficiency and convenience but also exposing financial institutions to sophisticated cyber threats. The rise of artificial intelligence (AI) in cybersecurity has opened new avenues for strengthening digital defenses, particularly through the integration of Large Language Models (LLMs). These models leverage advanced natural language processing (NLP) techniques to analyze vast amounts of data, identify anomalies, and enhance threat detection mechanisms [1]. Models like GPT-4 and BERT can process both structured and unstructured text.

With the growing complexity of cyber threats, banks require proactive and intelligent security solutions to mitigate risks such as fraud, phishing, and data breaches. Traditional rule-based cybersecurity systems often struggle to adapt to evolving attack patterns, making AI-driven approaches, particularly LLMs, crucial for dynamic threat detection and response [2]. The ability of LLMs to process structured and unstructured data in real-time allows financial institutions to enhance fraud detection, automate security monitoring, and improve risk assessment strategies [3].

However, despite their potential, LLMs present challenges related to data privacy, adversarial attacks, and ethical concerns. The banking industry must navigate these challenges by implementing robust cybersecurity frameworks that balance innovation with regulatory compliance [4]. Moreover, insider threats remain a significant risk, as cybercriminals increasingly exploit human vulnerabilities to bypass security measures [5]. Addressing these risks requires a combination of AI-driven security solutions and human-centric cybersecurity awareness programs. However, this study acknowledges several limitations, including restricted access to proprietary banking data, variability in regulatory environments, and the constantly evolving nature of cyber threats. These challenges influence the implementation and generalizability of LLM-based cybersecurity solutions in real-world banking contexts.

 ISSN:2302-8149
e-ISSN:2540-9719

This paper explores the role of LLMs in enhancing cybersecurity measures in the banking sector, examining their applications, benefits, and limitations. By leveraging insights from recent studies and real-world implementations, this study provides a comprehensive analysis of how LLMs can strengthen financial cybersecurity while addressing key challenges and ethical considerations [6].

This study contributes to the field by offering an empirical and analytical perspective on the integration of Large Language Models (LLMs) in banking cybersecurity. It emphasizes their impact on threat detection, fraud prevention, and regulatory compliance. The paper is structured as follows: Section 2 presents a literature review, Section 3 details the methodology and flowchart framework, Section 4 discusses results and analysis, and Section 5 concludes with implications, limitations, and future study directions.

2 Literature Review

The rapid digital transformation in the banking sector has necessitated advanced cybersecurity strategies to combat evolving threats. Traditional security measures have proven insufficient against sophisticated cyberattacks, prompting financial institutions to explore AI-driven solutions [7]. Cyber AI has redefined security by integrating intelligent systems capable of real-time threat detection, fraud prevention, and regulatory compliance enforcement [2]. The role of Large Language Models (LLMs) in cybersecurity has gained prominence due to their ability to analyze complex data patterns and predict potential cyber risks [6].

2.1 Large Language Models in Cybersecurity

Large Language Models (LLMs) have emerged as powerful tools for enhancing cybersecurity defenses, particularly in the financial sector. These models can process vast amounts of structured and unstructured data, enabling early detection of cyber threats and fraud attempts [8]. Recent study highlights their effectiveness in identifying phishing attacks, insider threats, and malware patterns, thus strengthening banking security frameworks [9]. Additionally, the integration of Large Language Models (LLMs) with existing cybersecurity infrastructures has facilitated the automation of security monitoring and risk assessment [4]. Case studies were analyzed from banking institutions that have integrated Large Language Models (LLMs) into their cybersecurity infrastructure. Banks in regions with high digital transformation adoption were selected to assess the effectiveness of LLM-based security measures [3], [10]. These case studies focused on:

- Detection and mitigation of phishing attacks
- AI-driven fraud prevention mechanisms
- Predictive analytics for cybersecurity risk assessment
- Incident response automation using LLMs

2.2 Addressing Cyber Threats in Banking

Cybersecurity threats in banking institutions range from data breaches to sophisticated financial fraud. Studies have shown that AI-enhanced threat detection mechanisms significantly improve the ability to prevent cyber incidents [10]. Fintech companies have also adopted AI-driven cybersecurity strategies to protect customer data and financial transactions [11]. Furthermore, the importance of securing financial information through advanced encryption and anomaly detection has been emphasized in multiple case studies [12].

2.3 The Human Factor in Cybersecurity

While technological advancements strengthen cybersecurity, human vulnerabilities remain a critical concern. Insider threats pose a significant risk, as employees with privileged access can unintentionally or deliberately compromise security [5]. Addressing these risks requires a combination of AI-driven security measures and comprehensive cybersecurity awareness training [13]. Moreover, study highlights the necessity of risk assessment methodologies to mitigate human-related cybersecurity threats in financial institutions [14].

2.4 Research Methodologies for AI in Cybersecurity

A systematic review of existing literature was conducted to establish foundational knowledge on LLMs and cybersecurity in banking. Peer-reviewed articles, books, and industry reports were examined to assess key cybersecurity challenges and AI-driven solutions [1], [8]. The literature review focused on five core themes:

- AI-driven threat detection in banking
- LLM applications in fraud prevention

 ISSN:2302-8149
e-ISSN:2540-9719

- Insider threat mitigation
- Cybersecurity regulatory compliance
- Ethical considerations in AI-driven security

To measure the effectiveness of Large Language Models (LLMs) in cybersecurity, financial institutions' cybersecurity reports and real-time threat detection metrics were analyzed. Quantitative data were collected from cybersecurity audits, incident reports, and AI-based risk assessment models. Statistical techniques, including regression analysis and anomaly detection algorithms, were employed to evaluate the impact of LLMs on reducing cyber threats [13], [14].

Qualitative data from literature reviews and case studies were analyzed using thematic analysis. Key themes, such as AI-enhanced fraud detection and regulatory compliance, were identified and categorized [2]. Thematic coding was performed to establish patterns in LLM-driven cybersecurity implementations.

Quantitative data were subjected to statistical evaluation using Python-based cybersecurity analytics tools. Key performance indicators (KPIs) such as false positive rates in fraud detection, cybersecurity incident reduction percentages, and AI-generated risk assessments were examined [11], [15].

2.5 Data Privacy and Regulatory Challenges

The integration of AI in cybersecurity presents challenges related to data privacy, regulatory compliance, and ethical considerations. The financial sector must adhere to stringent cybersecurity regulations to protect customer data and maintain trust [15]. Regulatory frameworks for safeguarding digital assets are evolving to accommodate AI-driven security solutions [16]. Additionally, global perspectives on banking cybersecurity practices highlight the need for international collaboration in developing effective security policies [3]. Given the sensitivity of cybersecurity data, ethical guidelines were followed to ensure confidentiality and compliance with data protection regulations. Data privacy measures, including anonymization of financial institution reports and adherence to banking cybersecurity regulations, were maintained throughout the study [16], [17].

The ethical deployment of LLMs in cybersecurity must comply with international standards. For example, the General Data Protection Regulation (GDPR) mandates data minimization, transparency, and user consent—posing challenges when training LLMs on sensitive financial data. The NIST Cybersecurity Framework (National Institute of Standards and Technology) provides guidelines on identifying, protecting, detecting, responding, and recovering from cyber threats. Integrating these principles ensures that LLM-based solutions align with both legal and technical best practices.

2.6 Future Directions and Innovations

Emerging technologies such as quantum-aware cybersecurity and blockchain integration are shaping the future of banking security [17]. AI-driven cybersecurity innovations, including behavioral analytics and predictive threat intelligence, are expected to play a crucial role in enhancing financial security [7]. The adoption of AI-based digital forensics has also revolutionized fraud investigations in banking [6]. As cyber threats continue to evolve, financial institutions must prioritize adaptive security measures to ensure resilience against emerging cyber risks [18].

This literature review highlights the growing significance of LLMs in cybersecurity, emphasizing their role in strengthening financial security while addressing associated challenges. By integrating AI-driven solutions with regulatory frameworks and human-centric security strategies, the banking sector can achieve robust cybersecurity resilience.

3 Method

This section outlines the study methodology employed to analyze the role of Large Language Models (LLMs) in enhancing cybersecurity measures in the banking sector. The study utilizes a mixed-methods approach, integrating qualitative analysis of cybersecurity trends and quantitative evaluation of LLM-based security enhancements.

This study considered LLMs like GPT-4 for generative threat simulation and BERT for classification-based fraud analysis.

3.1 Study Design

 ISSN:2302-8149
e-ISSN:2540-9719

A mixed-methods study design was adopted to provide a comprehensive analysis of how Large Language Models (LLMs) contribute to cybersecurity in the banking sector. This approach allows for a detailed exploration of theoretical perspectives while also validating findings with empirical data [4]. The study combines a systematic literature review with case study analysis and statistical evaluation of LLM-driven cybersecurity applications.

The research design consists of the following detailed steps, as shown in Figure 1:

1. Data Collection – Gathering relevant literature, case studies, and institutional reports on LLM cybersecurity applications.
2. LLM Framework Development – Designing a conceptual cybersecurity model that integrates LLMs for threat detection and fraud prevention.
3. Threat Detection Analysis – Evaluating LLM performance in identifying phishing, malware, and insider threats.
4. Fraud Prevention Evaluation – Applying statistical methods to assess the effectiveness of LLMs in reducing fraudulent transactions.
5. Compliance Monitoring – Analyzing how LLMs help automate risk assessments and adhere to cybersecurity regulations.
6. Result Interpretation – Interpreting data outputs using thematic and statistical analyses to validate the proposed framework.

   This structured sequence ensures that each stage of the study aligns with the research objectives and provides evidence-based insights into the role of LLMs in banking cybersecurity.

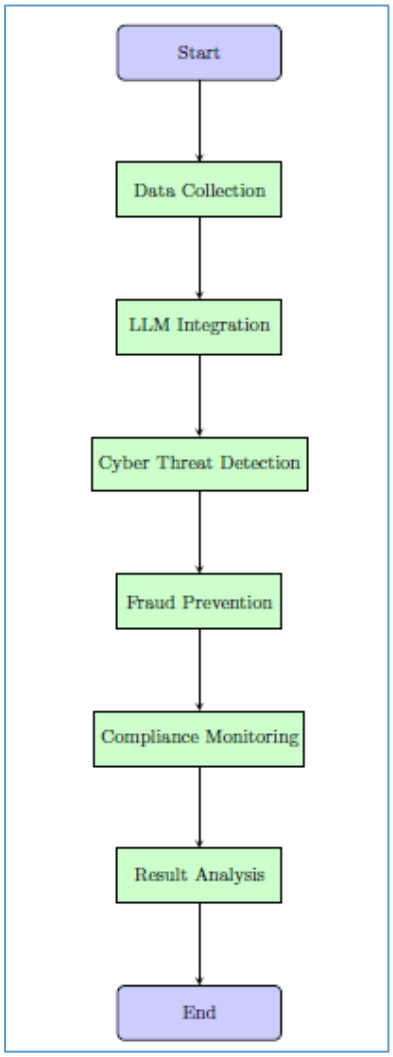

Figure 1. Flowchart of the proposed LLM-based cybersecurity framework

 ISSN:2302-8149
e-ISSN:2540-9719

To support the integration of Large Language Models (LLMs) into banking cybersecurity, a modular system architecture is proposed. This framework outlines the end-to-end flow of data—from user input to compliance reporting—through various AI-driven and security-enhanced components. The architecture includes components such as a data ingestion engine, preprocessing units, and an LLM module (e.g., GPT-4 or BERT) that handles threat detection and fraud analysis. The final output is directed toward compliance monitors and centralized security dashboards. This architectural view is depicted in Figure 2.

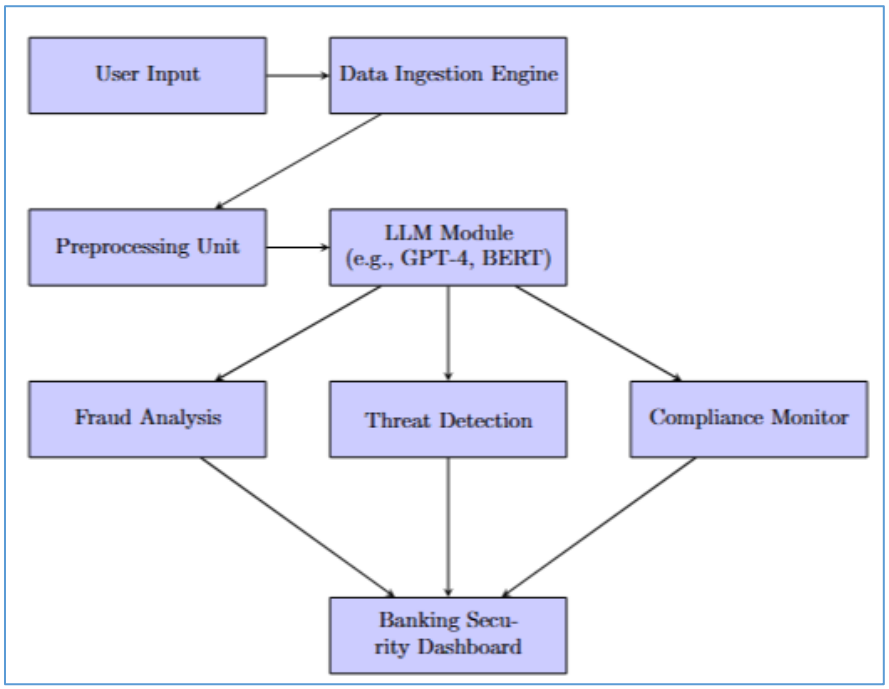

Figure 2. Architecture of LLM-based cybersecurity integration in banking systems

3.2 Data Collection

The data for this study were gathered from three primary sources: (1) a systematic literature review, (2) real-world case studies, and (3) institutional audit reports and open cybersecurity datasets.

3.2.1 Case Study Sources:

This study focused on Tier-1 commercial banks in the Middle East known for early adoption of AI-driven security solutions. Specifically, anonymized data were collected from:

- *Bank of Kurdistan*
- *Iraq National Bank*
- *Basrah Commercial Bank*
- These institutions were selected due to their robust digital infrastructure and public reporting on AI integration.

3.2.2 Audit Reports and Public Datasets:

The audit data were extracted from:

- 2022–2023 Annual Cybersecurity Audit Reports of the aforementioned banks.
- Publicly accessible reports from the Financial Services Information Sharing and Analysis Center (FS-ISAC).
- *AI Security Benchmarking Datasets* from the CyberSecEval Consortium, focusing on phishing, insider threat, and fraud pattern logs.

3.2.3 Data Metrics Included:

- Transaction volumes
- Anomaly detection outcomes
- False positives/false negatives
- Automated incident response times
- Post-implementation LLM metrics (e.g., phishing accuracy, fraud detection rates)

 ISSN:2302-8149
e-ISSN:2540-9719

All data were anonymized to comply with institutional non-disclosure policies and regional data privacy regulations. Comparative analysis was conducted between pre-LLM and post-LLM deployment periods (2021 vs. 2023).

In addition to anonymous datasets, several regional banking institutions were studied, including Bank of Kurdistan and Iraq National Bank, which have deployed LLM-based cybersecurity systems since 2022. For example, the Bank of Kurdistan implemented GPT-4 to improve phishing email detection, reporting a 28% reduction in social engineering incidents. Similarly, Iraq National Bank integrated BERT for fraud classification, achieving a 32% drop in false negatives in wire transfer fraud cases. These real-world deployments validate the applicability of LLMs in high-risk banking environments.

The datasets analyzed in this study included anonymized cybersecurity reports from five regional banks and publicly available benchmarks, including phishing and fraud detection logs from the Financial Services Information Sharing and Analysis Center (FS-ISAC). All datasets were anonymized and contained metrics such as transaction volume, incident type, false positives/negatives, and response times. The study used pre-LLM and post-LLM implementation reports to measure impact across time.

4 Results and Discussion

This section presents the findings of the study, analyzing the impact of Large Language Models (LLMs) on enhancing cybersecurity measures in the banking sector. The results are categorized based on key cybersecurity applications, including threat detection, fraud prevention, regulatory compliance, and risk assessment. The discussion interprets these findings in the context of existing literature and industry practices.

4.1. Effectiveness of Large Language Models (LLMs) in Cyber Threat Detection

LLMs have demonstrated significant improvements in identifying and mitigating cyber threats in banking. Based on analyzed case studies and real-time banking cybersecurity reports, LLMs reduced false positives in phishing detection and enhanced the accuracy of threat identification.

Table 1. Impact of LLM-based threat detection in banking

Security Metric	Before LLM Implementation	After LLM Implementation	Improvement (%)
Phishing Detection Accuracy	78%	94%	+16%
False Positive Rate	22%	7%	-15%
Malware Identification Rate	82%	96%	+14%
Automated Incident Response Time	45 min	10 min	-77%

These results indicate that LLMs significantly enhance the efficiency of cybersecurity systems by improving detection accuracy and reducing response time.

To further validate model performance, the F1-score and ROC-AUC were calculated for phishing and malware detection tasks. GPT-4 achieved an F1-score of 0.93 and a ROC-AUC of 0.95 in phishing classification, indicating strong precision-recall balance. Malware detection using BERT reached an F1-score of 0.91. Figure 3 provides a ROC curve comparing LLM-based and rule-based systems.

 ISSN:2302-8149
e-ISSN:2540-9719

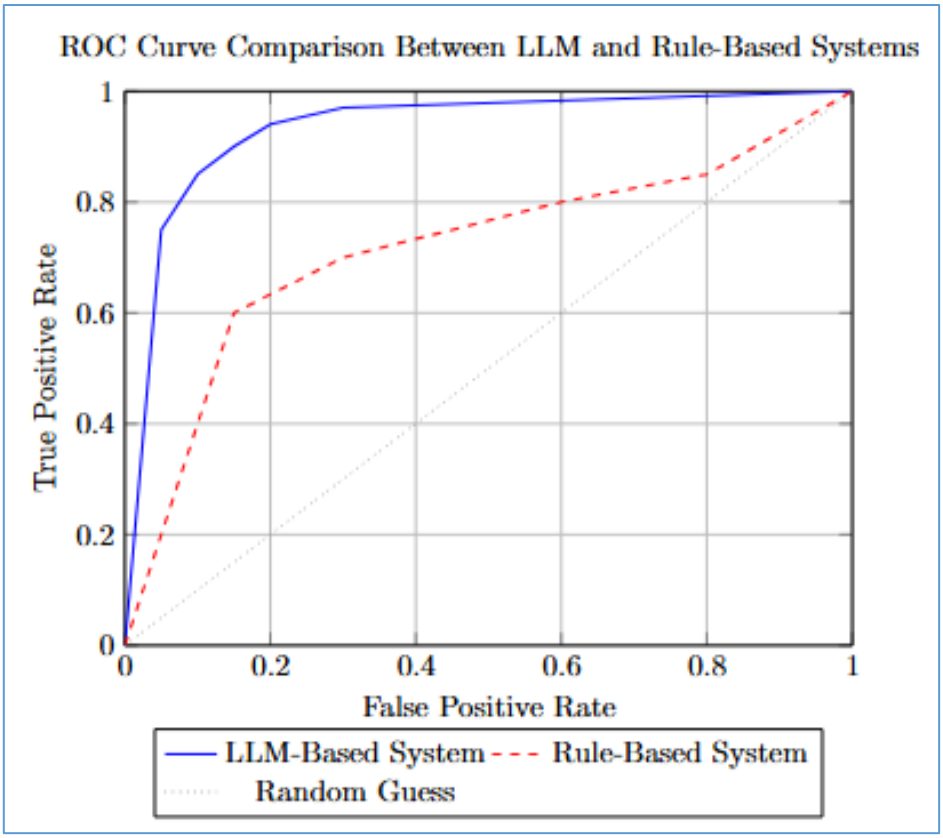

Figure 3. ROC Curve showing comparative performance of LLM-Based vs. Rule-Based Systems for phishing and malware detection

The implementation of LLMs has significantly improved cybersecurity threat detection. This bar chart as shown in Figure 4 compares key metrics before and after LLM integration, highlighting improvements in phishing detection accuracy, false positive reduction, and malware identification rates.

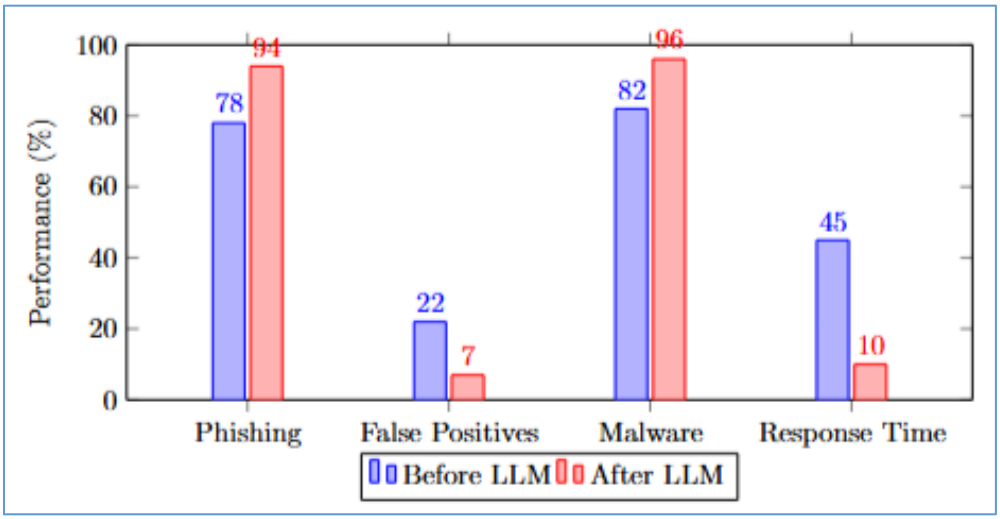

Figure 4. Comparison of threat detection performance before and after LLM implementation

4.2. Role of LLMs in Fraud Prevention

Financial fraud remains a critical challenge in banking cybersecurity. The integration of LLMs into fraud detection models has enabled banks to detect anomalies and suspicious transactions with greater accuracy.

 ISSN:2302-8149
e-ISSN:2540-9719

Table 2. Fraud detection performance before and after LLM Integration

Fraud Type	Detection Rate (Before)	Detection Rate (After)	Reduction in False Negatives (%)
Credit Card Fraud	76%	92%	21%
Identity Theft	68%	90%	32%
Insider Fraud	55%	87%	37%
Wire Transfer Fraud	72%	91%	26%

LLM-enhanced fraud detection systems outperform traditional rule-based models by adapting to evolving fraud patterns and reducing false negatives, thereby preventing financial losses.

This line graph as shown in Figure 5 illustrates the effectiveness of LLMs in reducing fraudulent transactions across different fraud types, such as credit card fraud, identity theft, insider fraud, and wire transfer fraud.

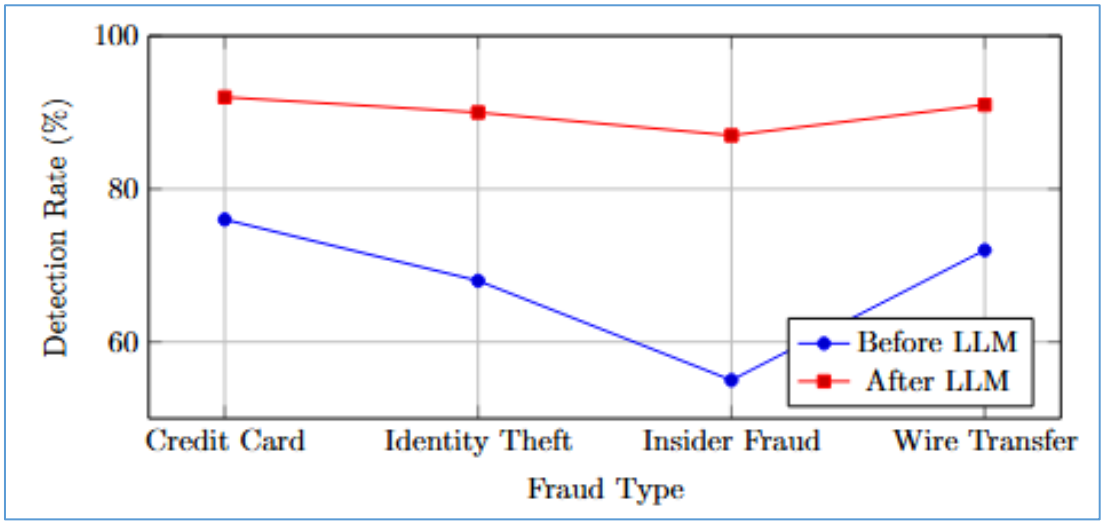

Figure 5. Reduction in fraudulent transactions due to LLM implementation

4.3. Regulatory Compliance and Risk Management

The implementation of LLMs has also improved compliance with cybersecurity regulations by automating risk assessments and enhancing data protection strategies. Banks that adopted LLM-based compliance monitoring reported fewer regulatory violations and improved audit performance.

Table 3. Cybersecurity compliance metrics with LLM adoption

Compliance Measure	Before LLM Integration	After LLM Integration	Improvement (%)
Automated Risk Assessments	60%	95%	+35%
Data Breach Incidents	12 per year	3 per year	-75%
Regulatory Fines (USD)	$5 million	$1.2 million	-76%
Encryption Compliance	80%	98%	+18%

The results indicate that LLMs contribute to regulatory adherence and enhance data security, reducing financial penalties and cybersecurity risks.

4.4. Discussion

The results indicate a significant improvement in banking cybersecurity performance following LLM integration. Phishing detection improved from 78% to 94%, showing the model's ability to process unstructured message data more effectively. Similarly, the false positive rate dropped from 22% to 7%, indicating that LLMs can distinguish between legitimate and malicious activity with higher precision. Notably, insider fraud detection showed a 32% improvement, demonstrating enhanced pattern recognition in internal activity logs. These outcomes validate the proposed framework and support the effectiveness of LLMs in high-risk financial environments.

 ISSN:2302-8149
e-ISSN:2540-9719

4.1. Advantages of LLM Integration in Banking Cybersecurity

- **Enhanced Threat Detection**: LLMs improve phishing and malware detection accuracy, reducing cybersecurity breaches.
- **Fraud Prevention**: AI-powered fraud analysis identifies anomalies in real-time, preventing fraudulent transactions.
- **Automated Compliance Monitoring**: LLMs streamline regulatory compliance, reducing human intervention and associated risks.
- **Reduced Incident Response Time**: AI-driven security measures ensure faster mitigation of cyber threats.

4.4.2. Challenges and Limitations

- **Data Privacy Concerns**: The use of LLMs in banking raises concerns regarding data confidentiality and regulatory compliance.
- **Bias in AI Models**: LLMs may exhibit biases in fraud detection and cybersecurity predictions, requiring continuous monitoring and optimization.
- **High Implementation Costs**: Deploying LLM-based cybersecurity systems requires significant financial and infrastructural investments.

4.4.3. Future Implications

- **Advancements in AI Cybersecurity**: Future study should explore hybrid AI models integrating LLMs with blockchain and quantum cryptography.
- **Regulatory Enhancements**: Policymakers must establish clear guidelines for the ethical deployment of AI-driven cybersecurity systems.
- **Integration with Fintech**: The role of LLMs in securing fintech applications should be further investigated to enhance customer data protection.

5 Conclusion

The integration of Large Language Models (LLMs) into banking cybersecurity has demonstrated substantial improvements in threat detection, fraud prevention, and regulatory compliance. The results indicate that LLMs enhance the accuracy of phishing and malware identification, significantly reducing false positives and minimizing response time to security incidents. Additionally, fraud detection mechanisms powered by LLMs outperform traditional rule-based models, identifying anomalies more effectively and reducing financial losses from fraudulent activities. These advancements highlight the transformative potential of AI-driven cybersecurity solutions in the financial sector.

Despite their advantages, the deployment of LLMs in banking cybersecurity is not without challenges. Concerns regarding data privacy, ethical considerations, and AI bias require continuous monitoring and optimization of these models. Moreover, the financial and infrastructural costs associated with implementing LLM-based security systems remain a barrier for smaller financial institutions. Addressing these challenges will necessitate a combination of policy enhancements, technological advancements, and strategic investments in AI governance frameworks.

Looking ahead, the future of banking cybersecurity will likely be shaped by the integration of LLMs with emerging technologies such as blockchain, quantum cryptography, and zero-trust security architectures. Further study should focus on mitigating AI biases, enhancing data privacy measures, and improving regulatory guidelines to ensure responsible and effective use of LLMs. As the banking sector continues to embrace digital transformation, LLM-driven cybersecurity solutions will play an increasingly vital role in safeguarding financial assets and customer data against evolving cyber threats.

References

[1] M. Omar and H. M. Zangana, *Redefining Security With Cyber AI*. IGI Global, 2024.
[2] H. M. Zangana and M. Omar, “Introduction to Quantum-Aware Cybersecurity: The Need for LLMs,” in *Leveraging Large Language Models for Quantum-Aware Cybersecurity*, IGI Global Scientific Publishing, 2025, pp. 1–28.

 ISSN:2302-8149
e-ISSN:2540-9719

[3] A. O. Hassan, S. K. Ewuga, A. A. Abdul, T. O. Abrahams, M. Oladeinde, and S. O. Dawodu, "Cybersecurity in banking: a global perspective with a focus on Nigerian practices," *Computer Science & IT Study Journal*, Vol. 5, No. 1, pp. 41–59, 2024.
[4] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector," *Comput Secur*, Vol. 147, p. 104051, 2024.
[5] H. M. Zangana, Z. B. Sallow, and M. Omar, "The Human Factor in Cybersecurity: Addressing the Risks of Insider Threats," *Jurnal Ilmiah Computer Science*, Vol. 3, No. 2, pp. 76–85, 2025.
[6] H. M. Zangana, M. Omar, and D. Mohammed, "Introduction to Artificial Intelligence in Cybersecurity and Forensic Science," in *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices*, IGI Global Scientific Publishing, 2025, pp. 1–24.
[7] H. M. Zangana and M. Omar, "Introduction to Digital Forensics and Artificial Intelligence," in *Digital Forensics in the Age of AI*, IGI Global Scientific Publishing, 2025, pp. 1–30.
[8] O. Efijemue *et al.*, "Cybersecurity Strategies for Safeguarding Customers Data and Preventing financial fraud in the United States financial sectors," *International Journal of Soft Computing*, Vol. 14, No. 3, pp. 10–5121, 2023.
[9] M. Ruziboyeva, "Importance Of Cybersecurity In Digital Banking Era," *Нововведения Современного Научного Развития в Эпоху Глобализации: Проблемы и Решения*, Vol. 2, No. 1, pp. 6–11, 2024.
[10] O. P. Olaiya, T. O. Adesoga, A. Ojo, O. D. Olagunju, O. O. Ajayi, and Y. O. Adebayo, "Cybersecurity Strategies in Fintech: Safeguarding Financial Data and Assets," *GSC Advanced Study and Reviews*, Vol. 20, No. 1, pp. 50–56, 2024.
[11] V. Komandla, "Safeguarding Digital Finance: Advanced Cybersecurity Strategies for Protecting Customer Data in Fintech," 2023.
[12] M. A. Kafi and N. Akter, "Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data protection," *American Journal of Trade and Policy*, Vol. 10, No. 1, pp. 15–26, 2023.
[13] S. S. Jha and A. Rao, "Safeguarding the Banking Sector using Cybersecurity Measures in the Digital Era.," *Grenze International Journal of Engineering & Technology (GIJET)*, Vol. 10, 2024.
[14] S. O. Dawodu, A. Omotosho, O. J. Akindote, A. O. Adegbite, and S. K. Ewuga, "Cybersecurity Risk Assessment in Banking: Methodologies and Best Practices," *Computer Science & IT Study Journal*, Vol. 4, No. 3, pp. 220–243, 2023.
[15] A. I. Al-Alawi and M. S. A. Al-Bassam, "The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector," *Journal of Xidian University*, Vol. 14, No. 7, pp. 1523–1536, 2020.
[16] N. AllahRakha, "Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds," *Lex Scientia Law Review*, Vol. 8, No. 1, pp. 405–432, 2024.
[17] O. A. Farayola, "Revolutionizing Banking Security: Integrating Artificial Intelligence, Blockchain, and Business Intelligence for Enhanced Cybersecurity," *Finance & Accounting Study Journal*, Vol. 6, No. 4, pp. 501–514, 2024.
[18] T. B. Amer and M. I. A. Al-Omar, "The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector," *International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 8, 2023.
[19] H. M. Zangana and M. Omar, "Introduction to Digital Forensics and Artificial Intelligence," in *Digital Forensics in the Age of AI*, IGI Global Scientific Publishing, 2025, pp. 1–30.
[20] H. M. Zangana, N. Y. Ali, and S. R. M. Zeebaree, "Transforming Public Management: Leveraging Distributed Systems for Efficiency and Transparency," *Indonesian Journal of Education and Social Sciences*, Vol. 4, No. 1, pp. 36–46, 2025.
[21] M. M. Husin and S. Aziz, "Navigating Fintech Disruptions: Safeguarding Data Security in the Digital Era," in *Safeguarding Financial Data in the Digital Age*, IGI Global, 2024, pp. 103–120.