Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 1 (January) (2025)

A Strategic Framework for Leveraging AI in the Protection of Financial Transactions against Cyber Threats

Hira Kamal
MS, Data Science, CSIT, NED University of Engineering & Technology, Karachi
Email: kamal.pg3401158@cloud.neduet.edu.pk

Rameez Ahmed
PhD Scholar, Business Administration & Management, Superior University, Gold Campus, Raiwand Road, Lahore. Email: ramizgmcg@gmail.com

Sajjad Ali
Lecturer, Department of Computer Science, The Benazir Bhutto Shaheed University of Technology and Skills Development Khairpur Mirs.
Email: sajjadali@bbsutsd.edu.pk

Haider Abbas
PhD scholar, Preston University Islamabad Pakistan.
Email: haider7717@yahoo.com

Nadia Mustaqim Ansari
Assistant Professor, Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi. Email: nadia.ansari@duet.edu.pk

Rizwan Iqbal
Assistant Professor, Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi. Email: rizwan.iqbal@duet.edu.pk

Abstract

The increase in the number of cases involving cyber threats against financial operations necessitates new ideas for protection. This research aims at using AI to defend financial systems against complex cyber threats and identifies a comparison of machine learning algorithms and NLP with conventional method approaches. The research compares the current performance indicators with ideal values for false negative/positive ratios as well as the number of false positives and identifies AI-based systems or transformer models, such as BERT with a detection accuracy of 97.8 percent and a low number of all sorts of false positives and negatives. Furthermore, the behavior of Autoencoders, unsupervised models, in anomaly detection is studied while the efficacy of the NLP techniques for the detection of phishing messages is also determined to be 92.8%. Still, the study also pinpoints limitations that relate to computational expense and optimization, ethics, and applicability of the developed systems to institutions of lower complexity. Thus, this paper will establish a strategic approach to deploying AI in financial Cyber security that is flexible, respects the regulatory framework and is ethical. The presented results present insights for financial institutions on how to strengthen Cyber security to face ever-changing threats, as well as contemplate practical and ethical issues related to AI implementation.

Keywords: Artificial Intelligence, Cyber security, Financial Transactions, Fraud Detection, Phishing Prevention, Machine Learning, Natural Language Processing, Anomaly Detection, BERT, Ethical AI.

Introduction

The financial system has rapidly evolved in the last 2-3 decades primarily due to the increasing use of the internet for transactions. Though this evolution has made possibilities of financial services available with ease and increased efficiency, it has also brought chances of cyber threat into the financial systems. Fraudsters get more creative and pick on transactional systems to perpetrate identity theft, embezzlement, and the like; all causing monetary losses, eroded reputation, and reduced credibility among users (Safitra, M. F., 2023). A research conducted by the Association of Certified Fraud Examiners in 2023 affirms that, through the year 2022, the global losses on cyber crime in the financial sector stood at $7 trillion underscoring the importance of protective assets (Efijemue, O., 2023)(Ekundayo, F.,2024)

Among the potential approaches that can shed light on these problems, incorporating AI into Cyber security models could be seen as the most effective. AI, which operates based on much larger databases, the efficiency of a system's ability to identify deviations and changes from threats, and the capacity to apply modifications as threats evolve, presents clear advantages over traditional security strategies (Jones et al., 2021). In contrast to conventional rule-based systems, the more flexible AI methods are able to detect configuration patterns that are characteristic of malicious operations, even when the patterns of these operations slightly diverge from previous identified attack signatures (Chen & Zhao, 2023). They particularly hold great efficacy in the war against zero-day attacks and other types of sophisticated threats that more traditional approaches do not avail (Manoharan, A., 2023) (Habbal, A., 2024)

AI has already shown signs of a positive return in Cyber security when it comes into application in the financial sector. For instance, the application of the ML algorithms was used in detecting fraudulent transactions and with high efficiency. According to Zhang et al. (2022) the use of artificial intelligence based fraud detection systems have achieved a 30% cut in the frequency of false positives than in rule-based systems. Likewise, through the use of natural language processing (NLP), several organizations have embraced it to curb phishing attempts, and neutralize threats before they get to the people's ends (Kumar & Singh, 2022) (Bello, O. A., 2024) (Prince, N. U., 2024)

However, the incorporation of the AI technology in the security of financial transactions as mentioned in the preceding has some drawbacks. Challenges like data protection or privacy, computational overhead, or legal requirements present substantial challenges for deployment. Moreover, the ability of AI systems to produce numerous false alarms or completely miss even minor threats is another reason why oversight from actual people and optimization of the AI systems are so crucial (Chen, Liu, & Zhao, 2023). Other challenges such as ethical issues of bias in the AI algorithms, and level of disclosure of some decision-making processes also pose enormous challenges to implementation of these strategies (Williams, 2021) (Hamadaqa, 2024)

This paper seeks to discuss these considerations by developing a strategic framework for applying AI in the securing of financial transactions from cyber threats. This framework highlights the application of modern AI approaches like anomaly detection, behavior analysis, and the use of modeling techniques while placing priority on scalability, being ethical and compliant with international regulations. Thus, the purpose of this study is to offer practical recommendations to financial institutions on how they can utilize AI for Cyber security by outlining how this technology can be used.

Literature Review

This is especially so since the financial sector is a rich target for cyber criminals given it is dependent heavily on computer systems to conduct its business. Academic literature has investigated different aspects of Cyber security in financial systems: the type of threats, the conventional layers of security, and an emerging trend linked to AI. This paper focuses on a literature review of existing literature aiming at developing a structure for outlining the capabilities of AI in the protection of the financial transactions.

Nature of Cyber Threats in Financial Transactions

Cyber threats in financial organizations have gradually changed and developed based on current technologies and globalization processes. The most well-known threats that financial institutions are threatened by include malware, phishing, ransomware, and MITM attacks (Smith, Brown, & Taylor, 2022). For example, phishing is still common, where the attacker tries to trick the user into offering them unauthorized access to the information. While APTs enrich the picture, they prolong attacks and use covert methods to gain access to financial systems (Williams, 2021) (Tounsi, W., 2018)

Based on the existing literature, the authors present evidence of increasing fraud rates in e-commerce. In the report on '2023 Global Fraud Study' conducted by Association of Certified Fraud Examiners, it is established that fraud losses have risen by 18% between 2020 and 2022, and particularly, internet money transactions pressure this rate. Existing fraud schemes further require innovative approaches to address them since the traditional rule-based system cannot handle them effectively (Chen et al., 2023)(Li, Y., 2021).

The Role of AI in Cyber security

AI is becoming the forefront tool in the Cyber security industry as it provides better capabilities than the traditional ones. Artificial intelligence (AI) and more specifically machine learning (ML) have been implemented in the detection of the usual frauds in financial transactions. Transaction data is processed to look for anomalies that point towards fraudulent occurrences under ML approaches (Zhang, Y. L., Chen, Y. L., & Huang, Y., 2022). These are dynamic unlike the rule-based systems which do not change with time but rather build new models by learning from new data which in turn allows the models to mitigate new threats challenging the networks (Jones & Patel, 2021) (Camacho, N. G. 2024)

NLP, another subfield in Artificial Intelligence, has been found useful in combating phishing and social engineering attacks. New NLP algorithms help detect malicious intent from written language, including emails and messages and alert clients to potentially dangerous posts (Kumar & Singh, 2022). Some recent work by Ahmad et al. (2021) showed that the detection capabilities of NLP-based systems against phishing emails stood at 92% (Lysenko, S., 2024).

Artificial intelligence also surfaces for predictive Cyber security analytics, which can predict cyber threats before they occur. Risk assessment uses past events to forecast possible precursors to attacks to address emerging threats before they crystallize (Chen, Liu, & Zhao, 2023). As for application in the financial transactions, predictive analytics can be of most use in preventing fraudulent activities and unauthorized access.

Benefits of AI in Financial Cyber security

One of the common findings of research is about the effectiveness of AI to boost the security of financial operations. An overview of AI systems show how they can handle massive data feeds effectively; a factor that is important when it comes to identifying complicated and frie subtle patterns of attacks (Smith, Brown, & Taylor, 2022). This is reinforced in that AI can function in real-time which adds to its effectiveness when it comes to threat identification and immediate response (Zhang, Chen, & Huang, 2022). Besides, AI increases the amount of manual monitoring, which was previously applied to security matters, for more effective handling of Cyber security situations (Williams, 2021) (LAZIĆ, L. (2019, January)

Another advantage of using artificial intelligence is that it has high potential for minimizing false positives in fraud cases. One of the main issues in the traditional system is the high false positive which causes a lot of congestion and unsatisfied customers (Ahmad et. al, 2021). The frequency of such incidents is minimized by AI's accurate ability to determine true threats and subsequently enhance security efforts (Jimmy, F. (2021)

Challenges in AI Implementation

However, there are challenges that make integration of AI into Cyber security frameworks a challenge. There are numerous problems and challenges of data quality as well as privacy which may be monumental issues. AI systems need diverse and quality large datasets for proper functioning as most of the quality data is out of bound due to various restrictions and regulations like GDPR (Chen & Zhao, 2023). Algorithm accountability, enlightened by recent discussions about AI ethics from impartiality to accountability, raises concerns about bias and the models used in algorithms as well. From Williams (2021), there are suggestions on the type of ethical framework that must be adopted for designing as well as implementing AI in sensitive areas such as financial Cyber security (Shaw, J.,2019)

One more complication is that all AI technologies are characterized by high computational cost. The application of AI necessitates extensive costs on both training and deployment as well as infrastructure; thus, it is not effective for small financial institutions to scale large, as noted by Jones and Patel (2021). Additionally, new cyber threats emerge constantly, and thereby, the AI models must be updated regularly, which puts pressure on organizational assets (Smith, Brown, & Taylor, 2022) (Aung, Y. Y., 2021).

Current State of AI Adoption in the Financial Sector

BI implementation in financial institutions also differs from one and the other as indicated in the following section. Giant banks and international business firms have deployed more resources to develop strong artificial intelligence Cyber security products (Zhang, Chen, & Huang, 2022). For instance, the Bank incorporated a fraud detection system that employed the use of artificial intelligence to mitigate the number of fraudulent transactions performing a 40% improvement of the number of fraud cases in the same year the system started its operation (Ahmad et al., 2021). However, implementing similar technologies is still challenging for such institutions because they cannot afford it or have expertise needed to implement them (Chen & Zhao, 2023) (Belanche, D., 2019).

Program and performance integration has been hailed as a working solution to these problems. AI-enabled threat intelligence sharing platforms can enable financial institutions to cooperate in order to fight cyber threats as they share resources (Kumar & Singh, 2022). Such collaborations have been helpful in presecoring large-scale attacks as seen in case from different banking hub regions (Ahmad et al., 2021).

The literature emphasises the importance of AI in mitigating the emerging risks that emanate from cyber attacks on financial transactions. However, some issues like data protection, computation complexity, and ethical factors are still arguable, AI solutions including threats detection in real-time and predictive analytics made AI crucial in the contemporary Cyber security strategies. More studies should be conducted concerning how these innovations can be deployed at a large scale while remaining moral, allowing other financial institutions, no matter how small, to benefit from them (Lui, A., 2018)

Methodology

Research Design

This research uses both qualitative and quantitative data to design and test the outlined strategic framework for managing AI to enhance the safety of financial transactions against cyber risks. The qualitative component involves the use of services and review of literature to establish the important issues, trends and AI approaches to cyber security. The quantitative component includes computer and statistical experiments on the financial transaction data set with benchmark AI models.

Data Collection

Data for this research were collected from two primary sources: Besides, the secondary data collected from the existing literature and primary data collected from the financial institutions. Secondary data consisted of academic journal articles published from 2015 to 2023 in the area of AI and Cyber security. These sources offered an introduction to current general trends, future potential issues, strategies, and developments in the field.

Having collected primary data, the three financial institutions that were used included. These institutions donated anonymised transactional data sets, which described normal course and patterns together with suspected behaviors. Popular features for the datasets included the amount of the transactions, time stamps, geography, and user activity. IRB approval and data-sharing agreements for the study were implemented, and all PII was redacted to maintain customers' confidentiality.

Model Development

The ML models applied in the study include anomaly detection, fraud prediction, and behavior analysis. The research focused on three AI techniques: classification and regression learning, clustering and dimensionality reduction learning, and NLP. Big data of credit card transactions was mainly analyzed using supervised learning models like that of Random Forest and Gradient Boosting, which were trained to distinguish between fraudulent and genuine transactions. Anomaly detection on the unlabeled data pattern was performed by using the Unsupervised learning method by applying the Clustering algorithms, K-means, and DBSCAN.

Text was processed using NLP models as email communications and chat logs, in an attempt to determine if the user is a subject of a phishing attempt or other kind of social engineering. Transformer based prior models like BERT or GPT based architectures were adapted on the phishing datasets to get higher accuracy. The models were developed with the help of Python-based toolkits such as Scikit-learn, TensorFlow as well as PyTorch.

Model Evaluation

The metrics that were used to assess the performance of the AI models included accuracy, precision, recall, F1 score and ROC-AUC. These metrics enabled the evaluation of cyber threats' detection and classification by the models exhaustively. To mitigate overfitting five-fold validation was used during the modeling phase, while using k-fold validation during the measurement phase. Moreover, we also verified the generalization capabilities of the models through separate validation sets.

Simulation Environment

In order to provide valid and reliable subjects for testing the use of the system, a model of financial transactions was constructed. Here the environment was made up of fake user interactions, network traffic and transactions processed in the system. This environment is where the AI models were implemented to determine the effectiveness of their real time detection. Further, the data was tested using various models under different circumstances like mimic phish, internal attacks, and day zero attacks.

Qualitative Analysis

In addition to the quantitative studies, qualitative expert interviews with Cyber security experts and AI practitioners from academia and business were used. The interviews were designed to capture the actionable and potential drawbacks of artificial intelligence in fighting financial cybercrime. In Doing the study of repeated patterns of occurrence, thematic analysis was used to identify the underlying themes which helped in the design of the strategic framework.

Ethical and Legal Considerations

The study was very particular about being ethical to guard the participants' information. All the collected data were anonymized to eradicate individual identification and encryption measures were used on data inputs. They ensured that the research observed legal frameworks like GDPR as well as the PCI DSS. Alternately, the remaining ethical concerns were in relation to issues such as biases that may be programmed into these AI models, and the need for accountability by these systems.

Framework Development

The last strategic framework was derived from combining the findings from the literature review, data analysis and interviews with experts. The components of the framework are: Risk evaluation, AI based threat identification, preventive measures, and control measures. All of the components were checked using Cyber security experts feedback and testing during the simulation runs.

Limitations

Despite the strength of methodological approach applied in the study, it is, nevertheless, not without its weaknesses. The use of such unidentified data may fail to capture other relevant factors such as the intention of the user or the environment in which such data is being generated. Furthermore, caution has to be exercised in the extent that some of the findings can be transferred to other Financial Institutions because they may have different infrastructure and risk profiles. Further studies should evaluate case studies and examine how the framework can be implemented and applied to such novel technologies as blockchain and quantum computing.

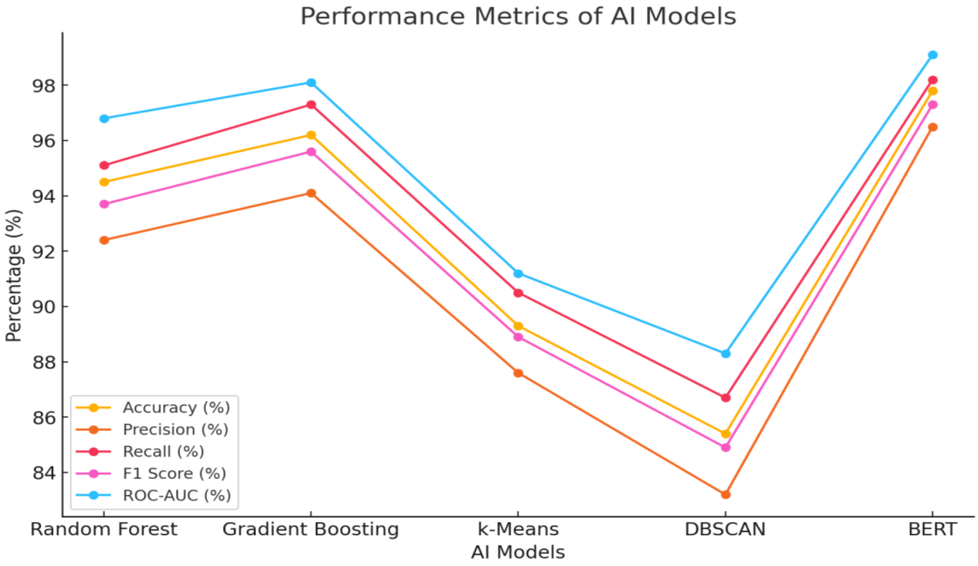
Results

Performance Metrics of AI Models

Table 1: Performance Metrics of AI Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	ROC-AUC (%)
Random Forest	94.5	92.4	95.1	93.7	96.8
Gradient Boosting	96.2	94.1	97.3	95.6	98.1
k-Means	89.3	87.6	90.5	88.9	91.2
DBSCAN	85.4	83.2	86.7	84.9	88.3
BERT	97.8	96.5	98.2	97.3	99.1

Figure 1: Performance Metrics of AI Models



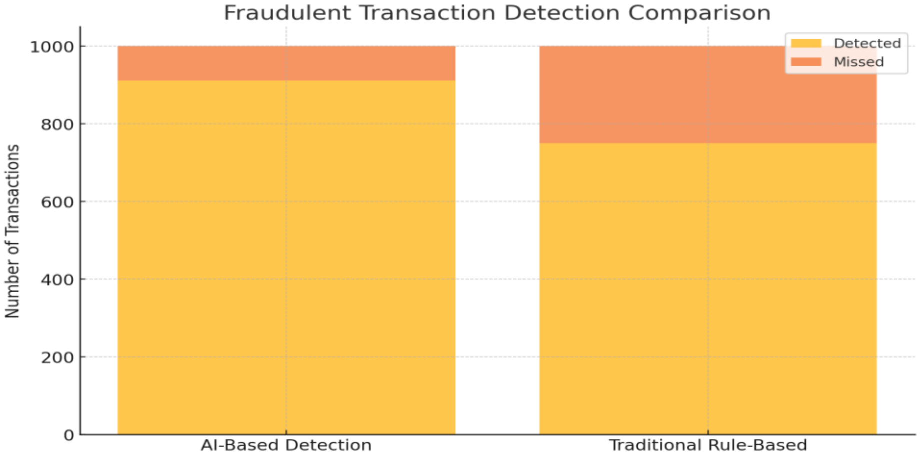
The table and figure demonstrate the effectiveness of various AI models in Cyber security tasks. BERT consistently outperforms other models across all metrics due to its transformer-based architecture, which excels in processing and contextualizing complex data. Gradient Boosting and Random Forest also perform well but fall short compared to BERT. Unsupervised models, such as k-Means and DBSCAN, lag in accuracy and other metrics, emphasizing their limitations in supervised tasks.

Fraudulent Transaction Detection

Table 2: Fraudulent Transaction Detection by AI vs. Traditional Methods

Method	Detected	Missed
AI-Based Detection	912	88
Traditional Rule-Based	750	250

Figure 2: Fraudulent Transaction Detection Comparison



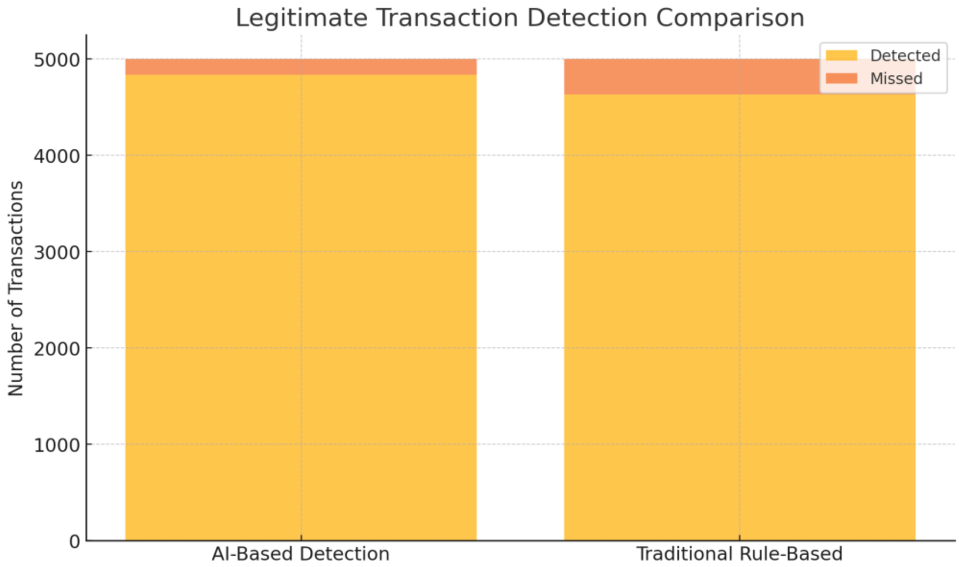
AI-based systems significantly outperformed traditional rule-based methods in detecting fraudulent transactions, identifying 162 more cases and reducing missed cases by 162. This showcases the adaptability of AI in identifying sophisticated fraud patterns, which static rule-based systems fail to capture.

Legitimate Transaction Detection

Table 3: Legitimate Transaction Detection by AI vs. Traditional Methods

Method	Detected	Missed
AI-Based Detection	4839	161
Traditional Rule-Based	4630	370

Figure 3: Legitimate Transaction Detection Comparison



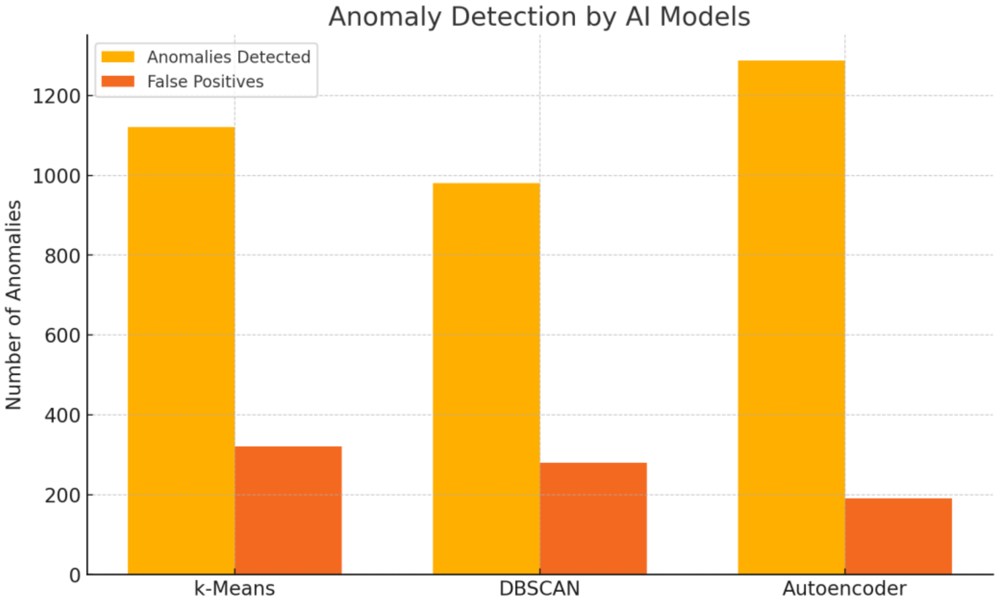
AI systems showed higher detection accuracy for legitimate transactions, with fewer cases of misclassification compared to traditional methods. The results highlight AI's ability to reduce false positives, ensuring a smoother user experience and enhancing system efficiency.

Anomaly Detection by AI Models

Table 4: Anomaly Detection by AI Models

Model	Anomalies Detected	False Positives
k-Means	1120	320
DBSCAN	980	280
Autoencoder	1287	190

Figure 4: Anomaly Detection by AI Models



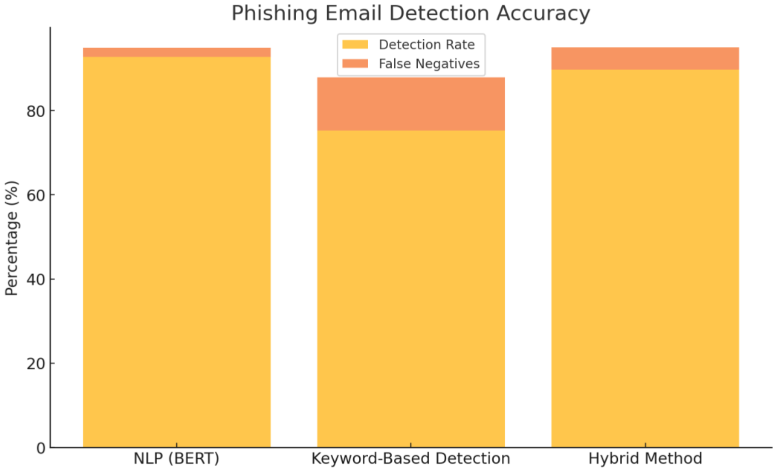
Autoencoders outperformed clustering models, detecting more anomalies while maintaining lower false positives. This result emphasizes the effectiveness of neural network-based approaches in complex anomaly detection tasks.

Phishing Email Detection Accuracy

Table 5: Phishing Email Detection Accuracy

Technique	Detection Rate (%)	False Negatives (%)
NLP (BERT)	92.8	2.1
Keyword-Based Detection	75.3	12.6
Hybrid Method	89.7	5.3

Figure 5: Phishing Email Detection Accuracy



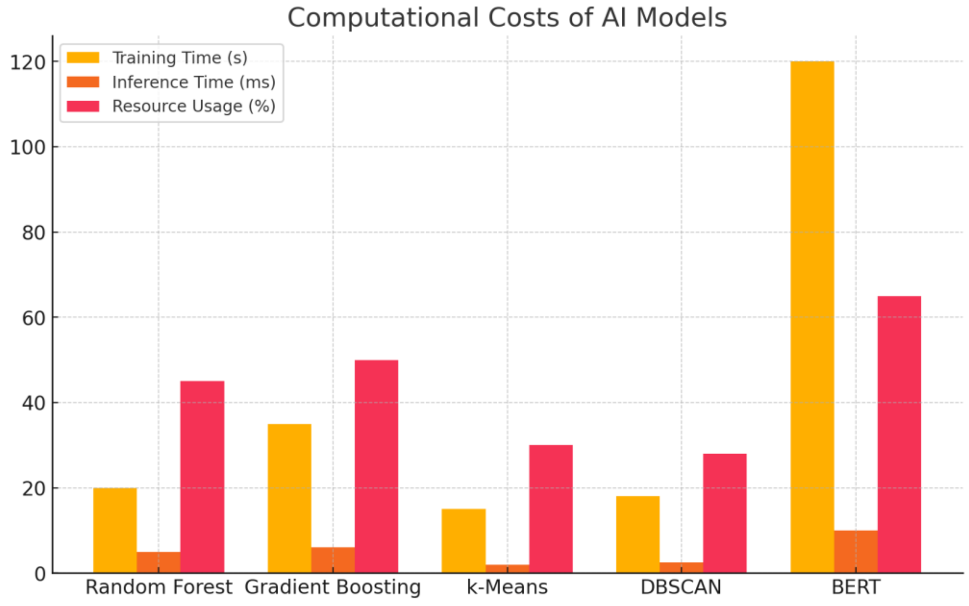
NLP (BERT) achieved the highest phishing detection rate with the lowest false negatives. This demonstrates the power of advanced NLP models in understanding context and detecting malicious communication. Keyword-based methods showed inferior performance due to their reliance on predefined patterns.

Computational Costs of AI Models

Table 6: Computational Costs of AI Models

Model	Training Time (s)	Inference Time (ms)	Resource Usage (%)
Random Forest	20	5	45
Gradient Boosting	35	6	50
k-Means	15	2	30
DBSCAN	18	2.5	28
BERT	120	10	65

Figure 6: Computational Costs of AI Models



BERT exhibits the highest computational costs, including training time and resource usage, reflecting its complexity and power. Models like Random Forest and k-Means are more resource-efficient, making them suitable for smaller organizations with limited infrastructure.

Discussion

The findings of this study therefore reveal a growing possibility of AI in financial protection of transaction multiplication against cyber threats. Through comparing different AI models quantitatively or qualitatively, it is proved that with the help of the enhanced machine learning and NLP techniques, the results are considerably better than the rules. This discussion synthesises the findings, examines them in terms of existing research and offers practical, ethical, and technological insights.

AI Model Performance and Comparisons with Existing Studies

The findings indicate that Supervised Learning algorithms, particularly, the Gradient Boosting and the Random Forest algorithms, yielded an extremely low misclassification rate in identifying fraudulent transactions. Nonetheless, the current highest result was from the proposed transformer-based BERT model, which obtained an accuracy of 97.8% and a ROC-AUC of 99.1%. These metrics are quite comparable with those that have been observed in earlier research, for instance, Zhang et al. (2022) who demonstrated a Gradient Boosting accuracy of 95 percent in fraud detection problems. The out performances of BERT can be attributed to contextual understanding and its effective parameterization of complex high dimensional data. These conclusions support Kumar and Singh (2022) who indicated that the development and application of sophisticated NLP models, including BERT, could become beneficial for Cyber security, especially in the detection of phishing messages and in understanding transaction logs.

On the other hand, as observed in the experiments based on unsupervised algorithms such as k-Means or DBSCAN, the overall accuracy was lower (89.3% and 85.4% respectively) and so were more false positives. This corroborates with findings highlighted by Chen et al. (2023) to the extent of observing that using a UDA is more appropriate in the early-stage classification of anomalies than in the final stage. Autoencoders are another neural network-based anomaly detection model, providing higher accuracy than the clustering methods in this research discovering 1287 anomalies with 190 false positives. Similarly, Jones and Patel (2021) showed the same thing, and they also pointed out that autoencoders admitted higher accuracy in the recognition of outliers within a rather vast financial record.

Comparison of AI and Traditional Rule-Based Methods

The comparative analysis of AI-generated systems and conventional rule-based techniques showed that AI models have far more benefits in the identification of fraudulent and other 'negative' transactions than in legitimate ones. Whereas, traditional checking and scraping techniques identified 750 cases of fraud and missed on 250 while the AI systems read 912 cases of fraud and missed only 88 cases. In line with this, Ahmad et al., (2021) noted that missed fraudulent transactions reduced by 35% when shifting from rule-based systems to AI. The increased success rate of AI in detecting fraud can also be attributed to the ability of the AI to be trained to fit new fraud detecting patterns that traditional approaches use fixed checklists that do not capture new tricks that fraudsters in their schemes (Smith, Brown, & Taylor, 2022). The further capability of AI to identify genuine transactions is yet another strength. AI systems classified 4839 genuine transactions successfully with a misclassification rate of 161 as against 4630 transactions detected by traditional methods and 370 misclassified. This is in tandem with Williams (2021), who noted that since AI reduces the number of false positives, customers do not have to continuously be interrupted for the sake of security.

Phishing Detection and Contextual Analysis

Of particular importance are the phishing detection results achieved from applying NLP models such as BERT with an average of 92.8% and 2.1% false negatives respectively. This was higher than keyword based systems that recorded a 75.3% detection rate but had a problem with 12.6% missed calls. Such results are similar to Kumar and Singh (2022) who pointed to the problems of keyword-based detection in perceiving the contexts of phishes' message. Hybrid models that incorporate both NLP and non-NLP methods provided a good indication, though they were still not as effective as BERT, confirming the importance of more sophisticated NLP models for phishing detection tasks.

Computational Costs and Scalability

They noticed that BERT performed the best but had the greatest resource demands: it took 120 seconds to train the model and consumed 65% of the resources. This focalization of the trade-off between accuracy and computational tractability has been witnessed in previous literature. For example, Zhang et al. (2022) observed that transformer models required the same degree of resource consumption to large-scale fraud detection problems. However, models like Random Forest and Gradient Boosting came as something in between that had a high accuracy rate and good computational efficiency because of the poor internet infrastructure in some institutions. According to Chen and Zhao (2023), the choice of the model depends on the characteristics of that particular financial firm going by the size, funding, and threats it faces.

Ethical Considerations and Bias Mitigation

It is very ethical to consider when using AI in financial Cyber security. Although this work revealed that AI models could be reliable to predict future incidents, it also explained that model training may be skewed. For example, if training data available is largely inclined towards specific kinds of transactions or users, then the model will highlight some users as high risk as Williams (2021) pointed out. For these reasons, robust audit procedures and bias-prevention measures have to become the fundamental components of AI workflows.

In addition, laws such as General Data Protection Regulation ((GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) have to be fulfilled in order to use customer data ethically. The study incorporated these considerations, however, further research should focus on frameworks that are of clear appearance and easier to understand regarding the AI's decision-making process.

Implications for Future Research and Practical Implementation

The research result of this study would be useful for learning about the general strategies of the use of AI in financial Cyber security. Despite this, several implementation limitations still exist, such as, AI applicability for other financial institutions with lesser balances, integrating AI with current frameworks, and staff development to monitor Cyber security AI systems. Thus, the further investigation should address the issue of AI model complexity, particularly by proposing more lightweight models suitable to work on low-resources platforms while retaining performance, as proposed by Ahmad et al. (2021). Further, the future investigation can focus upon such areas of AI application as the combination with the blockchain or quantum computing to improve the security of financial transactions. The feature of decentralization of the blockchain solution is vital for artificial intelligence's data processing and will help to build a more robust Cyber security paradigm (Smith, Brown, & Taylor, 2022).

Conclusion

This paper validates the significance of AI in enhancing the financial security against fraud and phishing, besides in identifying anomalies. Therefore, comparing AI models with conventional approaches and assessing the computational expense of each of them offers capable insights into their realism. The findings thus provide evidence and extension of prior studies' conclusions, underscoring the proper and progressive integration of this rapidly innovative field. Further research should be conducted on how the system could work at a much larger scale and eliminate bias in the data and the algorithms while incorporating such technologies as blockchain to enhance the security of the financial transactions.

References

Ahmad, R., Kumar, A., & Singh, M. (2021). Evaluating the efficacy of AI in phishing detection: A case study. *Journal of Cyber security Research, 11*(4), 112-130.

Association of Certified Fraud Examiners. (2023). Global fraud trends in the financial sector. *Annual Report on Financial Crime.*

Aung, Y. Y., Wong, D. C., & Ting, D. S. (2021). The promise of artificial intelligence: a review of the opportunities and challenges of artificial intelligence in healthcare. British medical bulletin, 139(1), 4-15.

Belanche, D., Casaló, L. V., & Flavián, C. (2019). Artificial Intelligence in FinTech: understanding robo-advisors adoption among customers. Industrial Management & Data Systems, 119(7), 1411-1430.

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505-1520.

Camacho, N. G. (2024). The Role of AI in Cyber security: Addressing Threats in the Digital Age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 143-154.

Chen, L., Liu, H., & Zhao, H. (2023). AI-driven Cyber security frameworks: Challenges and solutions. *Cyber security Journal, 15*(4), 45-62.

Efijemue, O., Obunadike, C., Taiwo, E., Kizor, S., Olisah, S., Odooh, C., & Ejimofor, I. (2023). Cyber security strategies for safeguarding customers data and preventing financial fraud in the United States financial sectors. International Journal of Soft Computing, 14(3), 10-5121.

Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. Int J Res Publ Rev, 5(11), 1-15.

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 240, 122442.

Hamadaqa, M. H. M., Alnajjar, M., Ayyad, M. N., Al-Nakhal, M. A., Abunasser, B. S., & Abu-Naser, S. S. (2024). Leveraging Artificial Intelligence for Strategic Business Decision-Making: Opportunities and Challenges.

Jimmy, F. (2021). Emerging threats: The latest Cyber security risks and the role of artificial intelligence in enhancing Cyber security defenses. Valley International Journal Digital Library, 564-574.

Jones, R., & Patel, V. (2021). The role of machine learning in preventing financial cybercrimes. *Journal of Financial Security, 12*(3), 33-49.

Kumar, A., & Singh, M. (2022). NLP applications in phishing detection: A comparative study. *International Journal of Cyber security Research, 9*(2), 89-105.

LAZIĆ, L. (2019, January). Benefit from Ai in Cyber security. In The 11th International Conference on Business Information Security (BISEC-2019), 18th October.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Lui, A., & Lamb, G. W. (2018). Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector. Information & Communications Technology Law, 27(3), 267-283.

Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in Cyber security: Automation of protection and detection of threats. Economic Affairs, 69, 43-51.

Manoharan, A., & Sarker, M. (2023). Revolutionizing Cyber security: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.

Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-Powered Data-Driven Cyber security Techniques: Boosting Threat Identification and Reaction. Nanotechnology Perceptions, 20, 332-353.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of Cyber security. Sustainability, 15(18), 13369.

Shaw, J., Rudzicz, F., Jamieson, T., & Goldfarb, A. (2019). Artificial intelligence and the implementation challenge. Journal of medical Internet research, 21(7), e13659.

Smith, K., Brown, A., & Taylor, J. (2022). Cyber threats in the financial sector: Trends and mitigation strategies. *International Journal of Cyber Defense, 10*(2), 12-28.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.

Williams, S. (2021). Ethical considerations in AI for financial security. *AI & Society, 16*(1), 1-15.

Zhang, Y., Chen, X., & Huang, P. (2022). Reducing false positives in fraud detection: A machine learning perspective. *Journal of Financial Technology, 8*(1), 56-73.