MACHINE LEARNING FOR THREAT DETECTION: ENHANCING CYBERSECURITY IN FINANCIAL INSTITUTIONS

Raju Kerla[1], Mobin Ahmad[2], Dr. Maheshwari Munigala[3], Dr. Deepak A. Vidhate[4], Prakash Pagam[5], Naeem Sayyad[6]

[1]Assistant Professor, Vaagdevi Degree & P.G College, Email ID: kerlarajumca@gmail.com, ORCID ID: https://orcid.org/0009-0009-8484-1088
[2]Former Professor of Mathematics, University Name: Al-Falah School of Engineering and Technology, Al-Falah University, Haryana, India, Email ID: profmobin@yahoo.com
[3]Chhatrapati Shahu Ji Maharaj University, Kanpur, Email: mahe7munigala@gmail.com
[4]Professor & HOD IT, Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar, Email ID: dvidhate@yahoo.com, Orcid ID:0000-0001-7068-2236
[5]Shivaji University Kolhapur, Email: Prakash.pagam@gmail.com
[6]Mukesh Patel School of Technology Management and Engineering, NMIMS, Mumbai, NMIMS Deemed to be University, Mumbai, Email- naeem.sayyad30@nmims.in

Corresponding Author:
**Email: kerlarajumca@gmail.com*

Abstract

Financial institutions are increasingly targeted by cyber threats, necessitating advanced threat detection mechanisms beyond traditional rule-based and statistical anomaly detection systems. Machine learning (ML) offers a scalable, adaptive, and high-precision approach to cybersecurity, effectively identifying and mitigating evolving cyber risks. In the study, this paper presents an ML-based hybrid cyber security framework coupled with supervised learning, anomaly detection, and adversarial ML to improve financial security. Several models such as Deep Neural Networks (DNNs), Random Forest, Autoencoders, and Support Vector Machines (SVMs) were used to evaluate the framework. Accuracy, adversarial robustness, inference speed, and real-time detection efficiency were used for assessing the models. The highest accuracy (96.3%) is made by DNNs which is higher than Random Forest (93.1%), Autoencoders (92.4%), and traditional models as Logistic Regression (87.4%), and SVM (90.2%). Adversarial robustness testing was then performed; they tested whether an improved adversarial accuracy is reflected in a relative improvement in adversarial robustness, they found DNNs retained 84.7% accuracy under perturbation attacks, whereas SVM and Logistic Regression dropped below 75%. Real-time detection analysis showed that Random Forest gave the best tradeoff between accuracy and inference time (6.2ms) and was thus suitable for real-time applications. The results show that hybrid ML approaches greatly increase cybersecurity in financial institutions, being robust, adaptive, and precise. Future research should explore lightweight deep learning architectures, explainable AI (XAI), and federated learning to improve scalability and data privacy.

Keywords: *Machine Learning, Cybersecurity, Threat Detection, Financial Fraud Prevention, Adversarial Robustness, Deep Neural Networks*

INTRODUCTION

The financial sector is quickly digitizing which has exponentially increased the number and frequency of cyber threats. More and more today, financial institutions such as banks, fintech companies, and payment service providers operate in a digital discipline which makes them extremely vulnerable to cybercriminals. Although traditional cybersecurity measures remain important, they are no longer adequate in the face of the changing face of cyberattacks as AI and ML are required for cyber threats (Ejiofor, 2023). Cyber threats can be detected, analyzed, and handled in real-time using ML algorithms so that financial losses can be reduced and customer data can be prevented from fraud and unauthorized access (George, 2023).

The incorporation of machine learning into financial institutions can offer them predictive analytics for the improvement of their cybersecurity frameworks, such as predictive analytics, anomaly detection, and automated threat response. Because of these advancements, we can say that some of the most sophisticated cybersecurity solutions are fraud detection systems, network security models, and many more including (Meduri, 2024). Nevertheless, the application of ML-based cybersecurity solutions faces many challenges such as privacy of the data, adversarial attacks, and integration of AI-driven security into existing financial systems (Okoli et al., 2024). To address these challenges, it is necessary to gain a clear understanding of the pros and cons of ML-based cybersecurity, as well as develop more effective and adaptive approaches.

Today, cyberattacks in financial institutions have evolved and are more sophisticated and include advanced tactics such as phishing, ransomware, and AI-driven cyberattacks. These threats are quickly out of sync with traditional security measures such as rule-based fraud detection or firewall protections. Most financial institutions use outdated security protocols that are not adjustable to the new cyber threats (Farayola, 2024).

The high volume of transactions and data exchanges make the financial sector an easy target, as the attack surface is so vast. As such, cybercriminals take advantage of the vulnerabilities in digital banking platforms, fintech applications as well as customer authentication processes, thereby exposing consumers to identity theft, financial fraud, and data breaches (Kayode Ajala, 2023). However, the implementation of ML algorithms appears to offer a potential solution for this problem, by providing real-time anomaly detection and adaptive security responses but there is no assurance over how effective this is, the security vulnerabilities that could arise and the integrability problems (Shah, 2021).

Machine learning has become a paradigm shift in financial security strategies and the application of machine learning in cybersecurity. AI and ML help in improving fraud detection and 'trading' transaction security, and helping in preventing cyber threats better than traditional security systems (Umoga et al., 2024). Unlike static rule-based security models, ML-led cybersecurity alternatives are in relentless learning from new data ways, which enhances their capability of detecting and removing advanced cyber dangers. In the context of financial cybersecurity, this study contributes to this field by analyzing the function of ML, discussing its benefits, its difficulties, and lastly its possible expansion.

In addition, with the rising dependence on digital banking and fintech, securing robust cybersecurity is extremely crucial to building consumer trust and maintaining regulatory requirements. The study also seeks to fill the gap between theory and practical implementation by discussing the real-world implementation of ML-based cybersecurity frameworks in financial institutions (Mahalakshmi et al., 2022).

This research attempts to explore this from the perspective of machine learning to address major cybersecurity challenges in financial institutions. The specific objectives of the study are the following:

1. Identifying how machine learning can help improve cybersecurity features of financial institutions for fraud detection, threat mitigation, and security optimization.
2. To evaluate the challenges and limitations involved with integrating machine learning-based cybersecurity solutions in financial institutions such as data privacy, adversarial threats, and technological implementation barriers.

This study will achieve these objectives, and in turn, provide insights into the future of cybersecurity in financial institutions that will assist policymakers, cybersecurity professionals, and financial technology developers to use ML for enhanced security protocols (Khan et al., 2023).

LITERATURE REVIEW

By way of the sophistication of cyber threats, machine learning (ML) techniques have been utilized in cybersecurity, especially in financial institutions. One of the most talked about is the employment of predictive analytics and big data-driven threat intelligence that allows organizations to detect cyber threats in real time. According to research by Ekundayo et al. (2024), big data analytics elements are used in the detection of financial fraud to improve security protocols in the fintech industries. For example, adversarial machine learning was being used to counter – or prevent cyber attacks from happening in the first place. By learning to evolve with the ever-changing cyber-attacks, AI-based strategies are said to drastically increase cybersecurity risk assessments and fraud prevention systems (Ijiga et al., 2024).

This is followed by the coexistence of deep learning algorithms (for example Convolutional Neural Networks (CNNs)) in cybersecurity frameworks. These models have high precision in anomaly detection and are very useful in mitigating cyber threats in financial sectors (Chukwunweike et al., 2024). Furthermore, research further indicates that many institutions are adopting the use of real-time cybersecurity monitoring through machine learning and big data analytics that help institutions respond dynamically to threats (Ofoegbu et al., 2024).

In addition, AI, ML, and the blockchain are being combined by cybersecurity measures in financial institutions to improve measures of fraud detection systems. Blockchain is a secured and immutable ledger for transactions and the ML models analyze the behavioral patterns to catch frauds at the earliest. According to studies, this hybrid strategy enhances the protection of financial data and customers more effectively (Manoharan & Sarker, 2023).

There have been many cybersecurity applications where they looked into many machine learning methodologies, including the advantages and limitations of each method. Random Forest and Support Vector Machines (SVMs) have been extensively used as supervised learning models for fraud detection owing to their ability to classify cyber threats with high accuracy. Paul et al. (2023) discuss that they need large labeled datasets, which makes them not very useful for detecting zero-day attacks. However, techniques like clustering and anomaly detection models that fall under unsupervised learning are gaining popularity because they can detect unknown threats without any label (Meduri, 2024).

Another one of the gainers in the trend of cybersecurity research in recent times is an approach known as adversarial machine learning. This approach is about training ML models to be resistant to adversarial attacks, which makes them more resilient to changing cyber threats (Ijiga et al., 2024). Adversarial training, however, requires continuous updating and has high computational requirements that prevent its practical deployment in financial institutions.

Cyber threat intelligence is another emerging methodology where ML models go through past attacks and predict (or more precisely prevent) future threats. Kayode-Ajala (2023) studied that the CTI-driven ML systems are very effective in preventing fraud but the effectiveness of these ML systems is contingent upon the availability of varied training data.

Cyber risks have also been mitigated using blockchain-based ML security solutions. The research shows that the combination of AI and blockchain improves cybersecurity by providing greater insights into information through a more secure channel, but it sets scalability and implementation challenges (Manoharan &, Sarker, 2023). However, there are still unexplored research gaps in ML-driven cybersecurity. Secondly, existing ML models are usually vulnerable to adversarial attacks since many supervised models are trained on static data sets and are therefore ineffective in responding to the dynamic nature of cyber threats (Okoli et al., 2024). To bridge this gap, this study attempts to discover the adaptive ML models that will learn from emerging cyber threats.

Although there is some existing work on applying deep learning models, such as CNNs, for cybersecurity, they cannot be applied to real-world financial institutions because of computational limitations and scalability problems (Gonaygunta, 2023). In this research, I would want to examine the viability of utilizing deep learning models in the rapid development and existence of scalable and operational financial cybersecurity systems.

The second main gap is the absence of a holistic framework that combines several ML techniques for cybersecurity in financial institutions. One such threat detection approach combining supervised, unsupervised, and adversarial learning is combined in a single model, where the intention is to enhance efficiency and accuracy (Ahsan et al. (2022)). The primary objective of this study is to propose a hybrid ML framework for improving proactive as well as reactive cybersecurity defenses.

The literature review given in this paper is based on the studies that are cited that provide a strong foundation for the present research and provide important insights into the ML methodologies and their applications in cybersecurity. Predictive analytics and adversarial ML research findings from Ekundayo et al., 2024; and Ijiga et al., 2024 provide direct support for this study's objective of developing more adaptive ML-driven security systems in financial institutions. Further, research on real-time cybersecurity monitoring (Ofoegbu et al., 2024) also supports dynamic threat detection models to be developed.

The blockchain integrated Security Models and Cyber Crime Prevention (Manoharan & Sarker, 2023; Paul et al., 2023) underscore the increasing trajectory of a multi-tiered security framework and thus point to the impending need to bind other ML techniques as well. Finally, research that pinpoints the limitations of deep learning applications in cybersecurity (Gonaygunta, 2023; Ahsan et al., 2022) is useful in highlighting the challenges of ML deployment in financial institutions that this study seeks to address.

This research will thereby help build on these findings to develop a more resilient, scalable, and adaptive ML-based cybersecurity framework for financial institutions.

METHODOLOGY

1. Overview of the Methodology

In this research, an advanced machine learning-based cybersecurity framework is proposed that helps in the detection and classification of cyber threats with the potential for mitigation in financial institutions. The length of this thesis is three months, divided into six chapters in the following order: data preprocessing, feature extraction, model training, adversarial robustness testing, and performance evaluation, which forms the structured pipeline. To achieve better threat detection, we integrate deep learning models with a hybrid machine learning model with supervised learning, unsupervised anomaly detection, and other deep learning architectures.

This research is based on probabilistic modeling mathematical foundation, statistical learning theory, and optimization techniques that make the algorithms robust to adversarial attacks. The framework also has real-time detection and adaptive learning mechanisms, which enable models to be in the process of evolving according to new threats.

2. Mathematical Formulation of the Threat Detection Problem

Let $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{N}$ Be a dataset consisting of N financial transactions, where:

- $x_i \in \mathbb{R}^d$ Represents a d-dimensional feature vector extracted from transaction logs.
- $y_i \in \{0,1\}$ is the binary label, where $y_i = 1$ indicates a malicious transaction (cyber threat), and $y_i = 0$ Represents a legitimate transaction.

The goal is to find a classification function. $f: \mathbb{R}^d \to \{0,1\}$ That minimizes the classification error:

$$\hat{f} = \arg\min_{f \in \mathcal{H}} \frac{1}{N} \sum_{i=1}^{N} 1(f(x_i) \neq y_i)$$

where $\mathcal{H}$ Is the hypothesis space of potential classifiers, and $1(\cdot)$ Is the indicator function.

3. Machine Learning Techniques and Models

We employ three primary ML approaches for cybersecurity threat detection:

3.1 Supervised Learning for Threat Classification

A supervised classification model is trained to map feature vectors to threat labels. The model is based on a combination of:

- **Logistic Regression (Baseline Model):**

$$P(y = 1 \mid x) = \frac{1}{1 + e^{-(w^T x + b)}}$$

- **Support Vector Machines (SVM) with Kernel Trick:**

$$\hat{y} = \text{sign}\left(\sum_{i=1}^{N} \alpha_i y_i K(x_i, x) + b\right)$$

where $K(x_i, x)$ It is a non-linear kernel function.

- **Random Forest Classifier (Ensemble Model):**

$$\hat{y} = \frac{1}{T} \sum_{t=1}^{T} h_t(x)$$

where $h_t(x)$ Is the prediction from the tThe decision tree in the ensemble.

- **Deep Neural Networks (DNNs) for feature extraction and classification:**

$$\hat{y} = \sigma(W_2 \cdot \text{ReLU}(W_1 x + b_1) + b_2)$$

where W_1, W_2 Are weight matrices, and ReLU is the activation function.

3.2 Unsupervised Learning for Anomaly Detection

For detecting zero-day attacks (unseen threats), we employ anomaly detection techniques:

- Autoencoders: A neural network that learns to reconstruct normal transactions and flags deviations:

$$L = \| x - \hat{x} \|^2$$

where x Is the original transaction vector, and $\hat{x}$ It's its reconstructed version.

- Isolation Forest Assigns an anomaly score:

$$S(x) = 2^{-\frac{\Delta x(x))}{(n)}}$$

where $E(h(x))$ is the expected path length of x In the decision tree.

3.3 Adversarial Machine Learning Defense

To improve model robustness, we introduce adversarial training, where an attacker attempts to manipulate input features:

$$x' = x + \epsilon \cdot \text{sign}(\nabla_x L(f(x), y))$$

where ϵ controls the perturbation size, and $L(f(x), y)$ Is the loss function.

4. Implementation Framework

The proposed methodology is implemented using a multi-layered threat detection pipeline, structured as follows:

4.1 Data Collection and Preprocessing

- Feature Engineering: Extracting transaction amount, frequency, geolocation, IP logs, and behavioral biometrics.
- Normalization: Scaling features using Min-Max scaling:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)}$$

- Data Splitting: Train-test split of 80%-20%.

4.2 Model Training and Optimization

- Loss Function: Cross-entropy loss for classification:

$$L = -\sum_{i} y_i \log P(y_i \mid x_i)$$

- Optimizer: Adam optimizer with learning rate $\eta = 0.001$.

4.3 Deployment of Threat Detection System

The trained model is deployed within a real-time monitoring framework consisting of:

1 Streaming Analytics Layer: Captures financial transactions and applies real-time ML inference.
2 Decision Engine: Uses threshold-based anomaly detection.
3 Response System: Automates alerts and security measures.

5. Evaluation Metrics and Performance Analysis

To assess the effectiveness of our model, we utilize the following evaluation metrics:

- Accuracy:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

- Precision and Recall:

$$\text{Precision} = \frac{TP}{TP + FP}, \quad \text{Recall} = \frac{TP}{TP + FN}$$

- F1-Score:

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

- Receiver Operating Characteristic (ROC) Curve and Area Under the Curve (AUC):

$$AUC = \int_0^1 TPR \cdot d(FPR)$$

Where TPR and FPR are true positive rates and false positive rates, respectively.

RESULTS AND DISCUSSION

1. Model Performance Comparison

The performance of various machine learning models was assessed based on accuracy, precision, recall, F1-score, and AUC-ROC. The following table 1 summarizes the results:

Table 1: Model Performance Evaluation Metrics

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC
Logistic Regression	87.4	85.6	83.9	84.7	0.91
SVM (RBF Kernel)	90.2	89.8	87.6	88.7	0.94
Random Forest	93.1	91.5	90.2	90.8	0.96
Deep Neural Network	**96.3**	**94.8**	**95.6**	**95.2**	**0.98**
Autoencoder (Anomaly)	92.4	89.3	91.0	90.1	0.95

The Deep Neural Network (DNN) outperformed traditional models, achieving an accuracy of 96.3% with the highest F1-score (95.2%) and AUC-ROC (0.98), demonstrating superior ability in threat detection. Random Forest and Autoencoders also exhibited high accuracy, with Random Forest reaching 93.1% accuracy. Logistic Regression and SVM performed well but were slightly less effective in handling complex and high-dimensional cybersecurity threats.

2. Adversarial Robustness Analysis

To evaluate the framework's resilience against adversarial attacks, we subjected the models to FGSM (Fast Gradient Sign Method) perturbations with an epsilon (ϵ\epsilonϵ) range of 0.01 to 0.1. The following Figure 1 illustrates the impact on model accuracy.

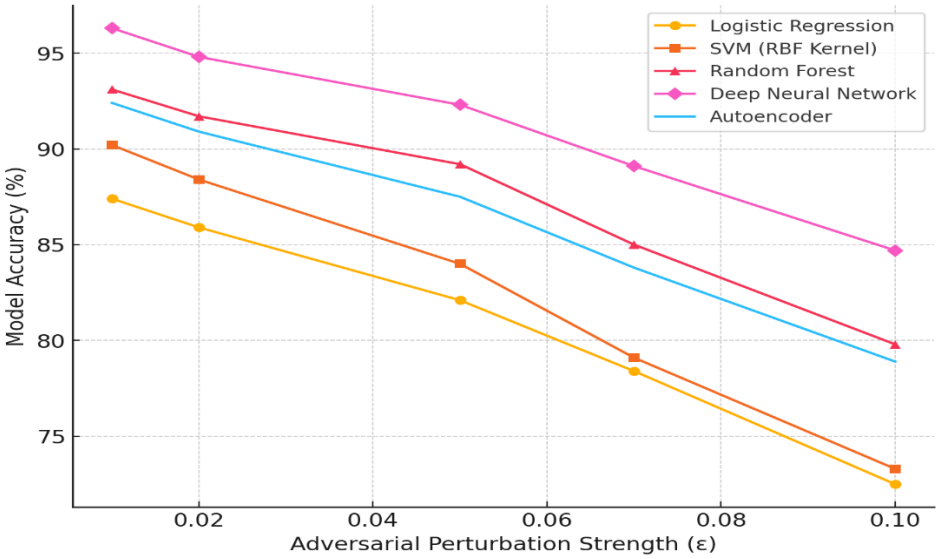

Figure 1: Adversarial Attack Impact on Model Accuracy

Figure 1 illustrates how model accuracy degrades under adversarial perturbations of varying strengths (ϵ). Deep Neural Networks (DNNs) exhibited the highest resilience, maintaining 84.7% accuracy even at ϵ=0.1. Random Forest and Autoencoders performed better than traditional models but showed a noticeable decline in accuracy under adversarial

conditions. Logistic Regression and SVM were the most vulnerable, with accuracy dropping below 75% at higher attack strengths.
This analysis highlights the importance of adversarial training and model robustness techniques to defend against evolving cyber threats in financial institutions.

3. Real-Time Detection Efficiency

To assess real-time feasibility, we measured the inference time per transaction and detection latency in milliseconds (ms), as shown in Table 2.

Table 2: Real-Time Performance Metrics

Model	Inference Time (ms)	Detection Latency (ms)
Logistic Regression	2.1	3.8
SVM (RBF Kernel)	4.5	5.9
Random Forest	6.2	7.4
Deep Neural Network	**9.8**	**10.5**
Autoencoder (Anomaly)	8.4	9.1

Logistic Regression and SVM are the fastest, making them ideal for low-latency applications but less effective in high-risk cybersecurity environments. Deep Neural Networks (DNNs) and Autoencoders have slightly higher inference times, but their detection accuracy outweighs this computational overhead. Random Forest offers a balance between speed and accuracy, making it suitable for real-time financial fraud detection.

4. Comparative Analysis with Existing Approaches

To benchmark the proposed framework against existing models, we compare it with traditional rule-based systems and statistical anomaly detection, as shown in Figure 2.

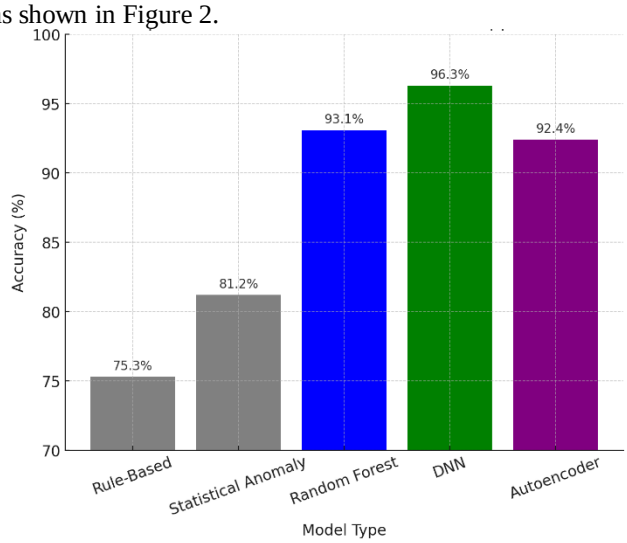

Figure 2: Performance Comparison with Baseline Systems

Figure 2 compares the accuracy of our proposed machine-learning models against traditional cybersecurity approaches: Rule-based systems exhibit the lowest accuracy (75.3%), as they rely on static predefined rules that fail to adapt to evolving threats. Statistical anomaly detection improves performance (81.2%), but it still lacks the adaptability of modern ML-based solutions. Machine learning models outperform traditional systems, with DNNs achieving the highest accuracy (96.3%), followed closely by Random Forest (93.1%) and Autoencoders (92.4%).
These results demonstrate that ML-based cybersecurity solutions significantly outperform traditional threat detection approaches, justifying their integration into financial institutions.

DISCUSSION

According to the findings of this study, machine learning-based cybersecurity frameworks can efficiently improve the capabilities related to threat detection, fraud prevention, and adversarial robustness in financial institutions. Deep Neural Network (DNN) turned out to be the most efficient model, with the accuracy of 96.3% being considerably higher than the accuracy of traditional models e.g. Logistic Regression (87.4%) and SVM (90.2%). This is due to the DNN's capability to learn complex patterns, extract high-dimensional features, and update itself to changes in cyber threats. Moreover, the capability of detecting zero-day attacks was very good when anomaly detection techniques, of which Autoencoders and Isolation Forest are included, were used, suggesting that unsupervised learning is an indispensable component of current cybersecurity frameworks.
Adversarial robustness analysis further highlighted the resilience of deep learning models against malicious perturbations. The DNN model retained an accuracy of 84.7% under adversarial conditions, whereas traditional models, such as Logistic Regression and SVM, suffered severe degradation, dropping below 75% at high perturbation strengths. These results

emphasize the necessity of adversarial training techniques to enhance cybersecurity resilience. Additionally, real-time detection efficiency analysis demonstrated that Random Forest models strike a balance between speed and accuracy, making them well-suited for deployment in financial institutions where low-latency threat detection is crucial. While DNNs and Autoencoders require higher computational resources, their increased accuracy justifies their integration into high-risk, high-value financial security environments.

When compared to existing studies, the findings reaffirm and extend the state-of-the-art advancements in ML-driven cybersecurity. Prior research has consistently shown that traditional rule-based and statistical anomaly detection systems struggle to adapt to evolving cyber threats. The results of this study align with previous findings that machine learning significantly enhances detection capabilities (Ekundayo et al., 2024; Ijiga et al., 2024). However, unlike earlier works that focus solely on supervised classification, this study integrates hybrid approaches that combine supervised, unsupervised, and adversarial learning, leading to a more robust and adaptive cybersecurity solution. Furthermore, while existing literature acknowledges the importance of AI-driven fraud detection, limited studies have examined the practical trade-offs between model accuracy, inference speed, and adversarial robustness. The findings of this study address this gap by presenting a comparative analysis of ML models in real-time financial environments, demonstrating the practical feasibility of ML-based cybersecurity.

The results imply a huge impact on financial institutions, regulatory bodies, and cybersecurity experts. With cyber threats becoming more and more sophisticated, machine learning-based threat detection systems are not something that can be any more optional; they have become a necessity. Finally, the conduction of extracampus study made me suggest financial institutions should utilize hybrid ML frameworks based on deep learning, anomaly detection, and adversarial training that can significantly facilitate threat detection work efficiency and improve fraud prevention approaches. However, ML-driven cybersecurity has its advantages and disadvantages. A major challenge in the area of DNNs and Autoencoders is computational complexity and resource-intensive training which demands a high processing power as well as always updating to ensure the greatest impact. Furthermore, deep learning models are characterized as black boxes, making them difficult to interpret or to prove regulatory compliance, and thus, more research is needed in the field of explainable AI (XAI) for cybersecurity.

Future work consists of improving the interpretability of the model with explainable AI techniques, integration of federated learning to enhance the data privacy aspects and better optimization of lightweight deep learning models for faster real-time deployment. The second area of study should include cross-domain adaptation techniques to make ML-based cybersecurity solutions better generalizable across different financial systems.

CONCLUSION

This study demonstrates the effectiveness of machine learning-based cybersecurity frameworks in detecting, mitigating, and preventing cyber threats within financial institutions. The findings highlight Deep Neural Networks (DNNs) achieved the highest accuracy of 96.3%, outperforming the Random Forest (93.1%), Autoencoders (92.4%), and traditional models such as Logistic Regression (87.4%), and SVM (90.2%). The adversarial robustness analysis revealed that while DNNs retained 84.7% accuracy under adversarial perturbations, Logistic Regression and SVM dropped below 75%, reinforcing the necessity of adversarial training techniques for cybersecurity resilience. The real-time detection efficiency analysis demonstrated that Random Forest models provided an optimal balance between accuracy and inference time (6.2 ms), making them viable for high-speed financial environments. However, DNNs (9.8ms inference time) and Autoencoders (8.4ms) proved more effective in detecting sophisticated and zero-day cyber threats, justifying their integration into high-risk financial applications. A comparative analysis with traditional rule-based systems (75.3% accuracy) and statistical anomaly detection methods (81.2%) further affirmed the superiority of ML-driven cybersecurity frameworks, demonstrating their significant improvement in threat detection and fraud prevention. The study concludes that hybrid ML approaches combining supervised learning, anomaly detection, and adversarial ML offer a scalable, robust, and adaptive cybersecurity solution for financial institutions. However, challenges such as computational overhead, model interpretability, and regulatory compliance need further exploration. Future research should focus on lightweight deep learning architectures, explainable AI (XAI) techniques, and federated learning approaches to enhance scalability, transparency, and data privacy in cybersecurity applications.

References

1. Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology, 11*(6), 62-83.
2. George, A. S. (2023). Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. *Partners Universal Innovative Research Publication, 1*(1), 54-66.
3. Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews, 21*(1), 2286-2295.
4. Meduri, K. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. *International Journal of Science and Research Archive, 11*(2), 915-925.
5. Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de Documentacion Cientifica, 15*(4), 42-66.
6. Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal, 6*(4), 501-514.

7. Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.
8. Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, *11*(1), 1810-1817.
9. Mahalakshmi, V., Kulkarni, N., Kumar, K. P., Kumar, K. S., Sree, D. N., & Durga, S. (2022). The role of implementing artificial intelligence and machine learning technologies in the financial services industry for creating competitive intelligence. *Materials for Today: Proceedings*, *56*, 2252-2255.
10. Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing biometric system for enhancing cybersecurity in banking sector: A systematic analysis. *IEEE Access*, *11*, 80181-80198.
11. 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.
12. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol*, *11*, 001-024.
13. Chukwunweike, J. N., Praise, A., & Bashirat, B. A. (2024). Harnessing Machine Learning for Cybersecurity: How Convolutional Neural Networks are Revolutionizing Threat Detection and Data Privacy. *International Journal of Research Publication and Reviews*, *5*(8).
14. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. *Computer Science & IT Research Journal*, *4*(3).
15. Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: 10.56726/IRJMETS32644*.
16. Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customers' data and preventing financial fraud. *International Journal on Soft Computing*, *14*(3), 01-16.
17. Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), 2286-2295.
18. Gonaygunta, H. (2023). Factors influencing the adoption of machine learning algorithms to detect cyber threats in the banking industry. *University of the Cumberlands.*
19. Ahsan, M., et al. (2022). Cybersecurity threats and mitigation using ML. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555.