International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 8, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i8.715

Adversarial Attack Detection in Banking Networks Using Ensemble Learning and AI

Giwa Olajumoke Sherifat[1]

Publication date 2025/08/27

Abstract

This research work explores the application of ensemble learning and artificial intelligence (AI) in detecting adversarial attacks in banking networks. Ensemble learning, a machine learning approach that combines the predictions of multiple models, can improve the accuracy and robustness of attack detection systems. AI-powered detection systems can analyze vast amounts of data in real-time to identify patterns and anomalies indicative of adversarial attacks. The article discusses the benefits and applications of ensemble learning and AI-powered detection in banking networks, including fraud detection, network security, and compliance. The authors recommend that banking institutions consider implementing these technologies to improve their cybersecurity posture and protect against evolving cyber threats.

I. INTRODUCTION

The banking sector is increasingly reliant on digital technologies to provide services to customers, making it a prime target for cyber-attacks (Oluwabusayo et al, 2023). Adversarial attacks, in particular, pose a significant threat to banking networks, as they involve sophisticated tactics designed to evade detection. Ensemble learning and artificial intelligence (AI) offer promising solutions for detecting and mitigating these attacks (Asma et al, 2023). This article explores the application of ensemble learning and AI in adversarial attack detection in banking networks.

II. ENSEMBLE LEARNING

Ensemble learning is a machine learning approach that combines the predictions of multiple models to improve overall performance (Asma et al, 2023). In the context of adversarial attack detection, ensemble learning can be used to combine the strengths of different models, each trained on different aspects of the data. By leveraging the diversity of multiple models, ensemble learning can improve the accuracy and robustness of attack detection systems (Asma et al, 2023). Techniques such as bagging, boosting, and stacking can be employed to create ensemble models that are better equipped to detect complex and evolving adversarial attacks.

The idea behind ensemble learning is to leverage the strengths of individual models and mitigate their weaknesses by combining their predictions. This approach has been widely adopted in various fields, including medical diagnosis, fraud detection, and sentiment analysis.

III. TYPES OF ENSEMBLE LEARNING

There are two primary types of ensemble learning:

- *Parallel Ensemble Learning:*

In this approach, multiple base models are trained independently on the same dataset, and their predictions are combined using a combiner. Examples of parallel ensemble learning include bagging and random forest.

- *Sequential Ensemble Learning:*

In this approach, base models are trained iteratively, with each model attempting to correct the errors made by the previous model. Examples of sequential ensemble learning include boosting and AdaBoost.

➢ *Combining Base Learners*

The combination of base learners is a critical step in ensemble learning. There are several techniques used to combine base learners, including:

- *Majority Voting:*

This involves assigning a vote to each base model, and the class with the majority vote is selected as the final prediction.

- *Weighted Majority Voting:*

This involves assigning weights to each base model based on their performance, and the weighted votes are used to determine the final prediction.

Sherifat, G. O. (2025). Adversarial Attack Detection in Banking Networks Using Ensemble Learning and AI. *International Journal of Scientific Research and Modern Technology*, *4*(8), 25–27. https://doi.org/10.38124/ijsrmt.v4i8.715

- *Other Combination Rules:*

Other combination rules, such as averaging, median, and product, can be used to combine the predictions of base learners.

➢ *Ensemble Selection*

Ensemble selection is a technique used to select a subset of base models that can lead to better performance than using all models. There are two primary approaches to ensemble selection:

- *Static Ensemble Selection:*

This involves selecting a single subset of base models during model training and applying it to predict all unseen instances.

- *Dynamic Ensemble Selection:*

This involves dynamically selecting a subset of models for making a prediction based on specific features of the unseen instances.

➢ *Benefits of Ensemble Learning*

Ensemble learning offers several benefits, including:

- *Improved Accuracy:*

Ensemble learning can improve the accuracy of predictions by combining the strengths of individual models.

- *Robustness:*

Ensemble learning can reduce the impact of overfitting and improve the robustness of predictions.

- *Handling Complex Datasets:*

Ensemble learning can handle complex datasets with multiple features and classes.

➢ *Applications of Ensemble Learning*

Ensemble learning has been applied in various fields, including:

- *Medical Diagnosis:*

Ensemble learning has been used to diagnose diseases such as heart disease, hypertension, and cancer.

- *Fraud Detection:*

Ensemble learning has been used to detect credit card fraud, advertisement fraud, and other types of fraud.

- *Sentiment Analysis:*

Ensemble learning has been used to analyze sentiments and opinions in text data (Ibomoiye and Yanxia, 2022)

IV. AI POWERED DETECTION

AI-powered detection systems can analyze vast amounts of data in real-time to identify patterns and anomalies indicative of adversarial attacks. The following sections outline the key components of AI-powered detection in banking networks.

➢ *Key Components of AI-Powered Detection in Banking Networks:*

- *Data Collection*

Effective adversarial attack detection requires access to high-quality data that captures the behavior of both legitimate and malicious activities (Prabin et al, 2024). Data collection involves gathering network traffic data, system logs, and user behavior data. This data can be used to train machine learning models to recognize patterns and anomalies associated with adversarial attacks (Asma et al, 2023).

- *Pattern Recognition*

Pattern recognition is a critical component of AI-powered detection systems (Oluwabusayo et al, 2023). Machine learning algorithms can be trained to recognize patterns in data that are indicative of adversarial attacks. These patterns can include unusual network traffic, suspicious user behavior, or anomalies in system logs (Asma et al, 2023). By recognizing these patterns, AI-powered systems can detect potential attacks and alert security teams.

- *Anomaly Detection*

Anomaly detection involves identifying data points that deviate significantly from expected behavior (Prabin et al, 2024). In the context of adversarial attack detection, anomaly detection can be used to identify unusual patterns or behavior that may indicate a potential attack. AI-powered systems can be trained to detect anomalies in real-time, enabling swift response to potential threats (Asma et al, 2023).

- *Predictive Analytics*

Predictive analytics involves using machine learning algorithms to predict the likelihood of future attacks based on historical data and trends (Oluwabusayo et al, 2023). By analyzing patterns and anomalies in data, predictive analytics can help identify potential vulnerabilities and weaknesses in the system. This enables security teams to take proactive measures to prevent attacks and improve the overall security posture of the banking network.

➢ *Benefits of AI Powered Detection*

AI-powered detection systems offer several benefits in detecting adversarial attacks in banking networks. These benefits include improved accuracy, reduced false positives, and enhanced scalability (Asma et al, 2023). AI-powered systems can analyze vast amounts of data in real-time, enabling swift detection and response to potential threats (Oluwabusayo et al, 2023). Additionally, AI-powered systems can learn from experience and adapt to evolving threats, making them a valuable tool in the fight against cybercrime (Prabin et al, 2024).

V. APPLICATION OF ENSEMBLE LEARNING IN BANKING NETWORKS

Ensemble learning has several applications in banking networks, including:

- *Fraud Detection*

Ensemble learning can be used to detect fraudulent activities in banking networks, such as credit card fraud or money laundering (Asma et al, 2023). By combining the predictions of multiple models, ensemble learning can improve the accuracy and robustness of fraud detection systems.

- *Network Security*

Ensemble learning can be used to detect and prevent cyber-attacks on banking networks (Oluwabusayo et al, 2023). By analyzing network traffic and system logs, ensemble learning models can identify potential security threats and alert security teams.

- *Compliance*

Ensemble learning can also be used to ensure compliance with regulatory requirements in banking networks (Oluwabusayo et al, 2023). By analyzing transaction data and identifying potential anomalies, ensemble learning models can help banks comply with anti-money laundering (AML) and know-your-customer (KYC) regulations.

VI. RECOMMENDATION

Based on the benefits and applications of ensemble learning and AI-powered detection, we recommend that banking institutions consider implementing these technologies to improve their cybersecurity posture. Specifically, we recommend:

- Investing in AI-powered detection systems that can analyze vast amounts of data in real-time (Oluwabusayo et al, 2023)
- Implementing ensemble learning models that can combine the predictions of multiple models to improve accuracy and robustness (Asma et al, 2023)
- Ensuring that AI-powered systems are designed with transparency and explainability in mind, to facilitate regulatory compliance and stakeholder trust (Prabin et al, 2024)

VII. CONCLUSION

In conclusion, ensemble learning and AI-powered detection offer promising solutions for detecting adversarial attacks in banking networks. By leveraging the strengths of multiple models and advanced analytics, these systems can improve the accuracy and robustness of attack detection (Asma et al, 2023). As the threat landscape continues to evolve, it is essential for banking institutions to invest in advanced security measures that can detect and mitigate complex cyber threats (Oluwabusayo et al, 2023). By adopting ensemble learning and AI-powered detection, banking institutions can enhance their security posture and protect against the evolving threat of adversarial attacks.

REFERENCES

[1] Asma A. A. et al (2023) An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures. Engineering, Technology & Applied Science Research Vol. 13, No. 6, 2023, 12433-12439

[2] Ibomoiye D. M. and Yanxia S. (2022) A Survey of Ensemble Learning: Concepts, Algorithms, Applications, and Prospects. Digital Object Identifier 10.1109/ ACCESS 2022.3207287

[3] Katya, E. (2023) Exploring Feature Engineering Strategies for Improving Predictive Models in Data Science. Research Journal of Computer Systems and Engineering, 4(2), 201-215.

[4] Olawale O. et al (2024) AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. GSC Advanced Research and Reviews, 2024, 21(02), 227–237

[5] Oluwabusayo A. B. et al (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, 2023

[6] Prabin A. et al (2024) Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive, 2024, 13(01), 1457–1472

[7] Sánchez P. M. S. et al (2021) A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. IEEE Communications Surveys & Tutorials, 23(2), 1048-1077.