Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

Leveraging Artificial Intelligence to Combat Cyber Threats in Financial Institutions

Santhosh Kumar Swayampakula

Independent Researcher, Wells Fargo (USA)

ARTICLE INFO

Received: 03 March 2026
Accepted: 04 April 2026
Published: 12 April 2026

ABSTRACT

The proposed study explores how artificial intelligence can be used to improve cybersecurity in financial institutions through machine learning, deep learning, and behavioural biometrics in the detection of fraud. It compares the models, including the Random Forest, Logistic Regression, Isolation Forest, and a deep-learning classifier. The mean reveals that Random Forest is better than Logistic Regression at an accuracy of 78% compared to 51% which is statistically significant (p = 3.37e-08). Nevertheless, none of the models can adequately detect fraudulent transactions indicating that it is quite challenging to identify fraud in real-time in financial ecosystems, and that AI-based detection systems still require further enhancements.

Keywords: Artificial intelligence, cybersecurity, financial institutions, machine-learning, deep-learning, Random Forest, Logistic Regression, Isolation Forest, deep-learning classifier, fraud-detection challenges, fraudulent deals, intrinsic limitations, financial ecosystem.

Introduction

Financial institutions are increasingly vulnerable to more advanced cyber-threat incidents, including ransomware, phishing, and insider attacks. The old traditional security measures cannot be used to mitigate these emerging risks any longer. Artificial Intelligence (AI) is one of the solutions that delivers state-of-the-art, real-time defense mechanisms. Machine learning, behavioral biometrics, and deep learning are artificial intelligence technologies that increase threat detection, fast detection of anomalies, and zero-day exploits [1]. This introduction discusses the ways AI can be incorporated into the cybersecurity measures to safeguard sensitive financial information and guarantee operational safety.

Research Aim

This study aims to conduct research to examine how Artificial Intelligence (AI) can be used to improve cybersecurity in financial institutions in terms of its effectiveness against advanced cyber-attacks.

Research Objectives

- *To evaluate the usefulness of AI-based threat detection systems within financial organisations.*
- *To determine how machine learning, behavioral biometrics, and deep learning can be used to detect cyber threats.*
- *To discuss the benefits and difficulties of the application of AI-based defense measures at the financial institutions.*

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Problem statement

Advanced cyber threats are increasingly targeted on financial institutions, with the ransomware attacks increasing by 30% within the last one year. Conventional cybersecurity solutions are failing to keep pace, thus the critical need to adopt AI-driven solutions that provide real-time detection and dynamic defense against dynamic threats and protect sensitive financial data.

Novel contribution

This study introduces a new strategy of using machine learning, deep learning, and behavioral biometrics to promote cybersecurity within financial organizations. In contrast to the literature, it is dedicated to the integration of such AI methods in order to detect threats in real-time and prevent attacks based on zero-day attacks [3]. The contribution is application and methodological in nature, which proposes a broad, dynamic defense strategy to reduce the risk and protect the sensitive data related to financial operations against the changing cyber threats.

Literature Review

AI-Driven Threat Detection Mechanisms in Financial Institutions

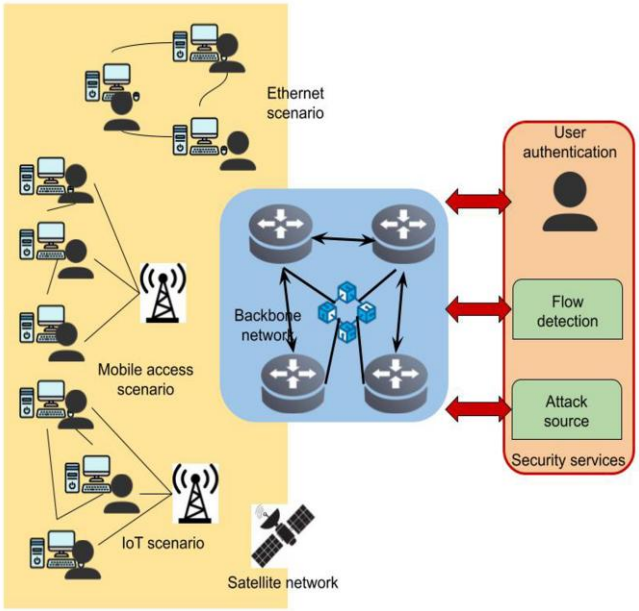

Fig. 1: AI-Driven intrusion detection and prevention systems

AI has been used to be a very critical instrument towards the current-day cybersecurity, especially in banking systems. As cyber-attacks have been on the increase, AI provides dynamic and automated defense solutions [4]. Artificial intelligence systems have the ability to scan large volumes of data and keep track of them continuously to identify possible threats in real-time [5]. As an example, machine-learning models are capable of monitoring transactional pattern, network traffic, and user behavior that may alert administrators to an unusual action [6]. In contrast to traditional systems, AI is able to detect and react to insecurities rapidly, even on those never experienced before since it learns through information over time.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

Machine Learning in Identifying Cyber Threats

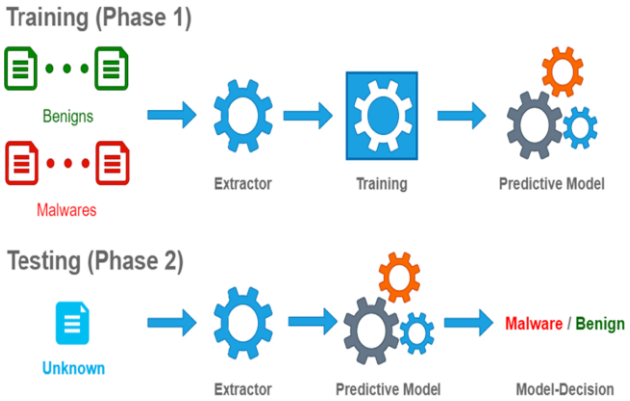

Fig. 2: Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity

One of the foundations of AI-based cybersecurity systems is machine learning. Machine-learning applications can detect irregularities in data, and, therefore, they can identify future threats at an early stage [7]. Under supervised learning, the labelled data are recognized to identify known threat kinds, whereas under unsupervised learning, the new, never-before-seen attack patterns are identified by identifying the outliers in the data [8]. Machine-learning-based anomaly detection finds application in financial institutions to detect suspicious transactions or fraud in bank accounts by identifying variation in the pattern of behavior [9]. Such systems are also able to categories network traffic thereby separating between normal and malicious activity thereby enhancing real time intrusion detection [10]. Also the machine learning allows predictive threat modelling whereby the former attack experiences are utilized to predict the future occurrence of threats, that guides the financial institution to prepare for any future attack [11]. These systems learn automatically through their ever-evolving data and become increasingly effective in detection and alleviation of threats.

Behavioral Biometrics in Cyber Defense

Fig. 3: Behavioral Biometrics for Fraud Detection

Behavioral biometrics involves the use of AI in the constant authentication of users with uniqueness in the pattern of their interaction on features like keystroke, mouse pattern, and touch gestures [12]. Such an approach offers constant active authentication that becomes much more challenging to fake than either a general password or two-factor authentication systems [13]. Behavioral biometrics is used to increase security in the case of the financial institution since it identifies deviant behavior that may be an indication of fraud or unauthorized entry [14]. The AI can identify the difference between the normal patterns of interaction of a person and warn the administrator about the possible account violation or insider threat

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

[15]. This two-way security layer is especially important in prevention of frauds and in the protection of sensitive financial information being accessed solely by authorized users [16]. Nevertheless, there are still issues with guaranteeing the validity of such systems among varying demographics and the users behavior.

Deep Learning in Advanced Threat Detection

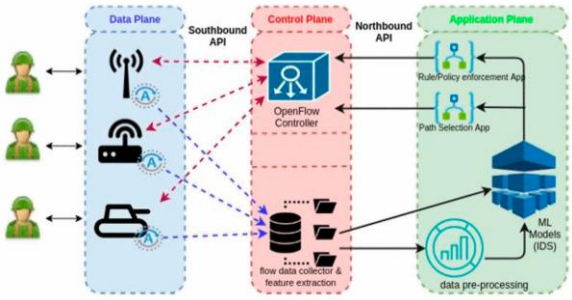

Fig. 4: Network Threat Detection Using Deep Learning

Deep learning, is a branch of machine learning, is well adaptable to handling large and complicated data [17]. This makes deep learning unlike traditional methods as it can analyses complex patterns in unstructured data: network traffic, emails, transaction logs, etc. [18]. Deep-learning algorithms, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can be used in financial organizations to analyses time-series data to detect a threat, including phishing or advanced persistent threats (APTs) [19]. As an example, deep-learning can track real-time transaction patterns and identify anomalous spending patterns or malware [20]. They are also able to identify phishing attacks not only based on email content but also structure [21]. Deep learning can be used as a potent tool to detect and mitigate threats in real-time due to its capacity to use mass datasets and enhance its efficacy.

Benefits and Challenges of AI-Based Defense Strategies

The implementation of AI in the efforts of financial cybersecurity has various advantages. By increasing the speed and precision of the detected threats, AI allows responding to threats in real time [22]. With machine learning and deep learning, it is possible to process data in large quantities, detect habits, and anticipate any possible attack and enhance the overall security efficiency [23]. Behavioral biometrics provide a higher degree of security where only the legitimate users can access accounts [24]. Nevertheless, it is problematic to implement AI-based defense measures [25]. Initial expenditure on installation of AI systems is large and financial institutions need to invest in the required developments and talented individuals to handle these systems [26]. Furthermore, AI models are very successful; however, it does not make them impossible to inaccurately identify false positives and misdiagnoses [27]. The financial institutions have to strike the balance between the advantages of real time detection of threats and possible system overloading because of false alerts [28]. There is also a challenge on regulatory and compliance issues [29]. The financial institutions should make sure that AI systems do not violate the data protection laws like GDPR [30]. An AI model has to be trained with the help of the data that is secured, and the data must be anonymized to guarantee customer privacy, that requires effective data governance initiatives.

Literature gap

Studies that apply AI models, such as the Random Forest, Logistic Regression, and Isolation Forest to detect fraud, can be compared in the literature review. Indicatively, although a single user showed that the use of Random Forest is promising in detecting frauds, their work is inadequate in dealing with fraudulent transactions. Conversely, in a different study that investigated anomaly detection, however, without using

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://jisem-journal.com/ Research Article

behavioral biometrics as a factor of real-time fraud prevention [31]. The research fills this gap through the combination of AI-based solutions to transactional behavior analysis and ongoing authentication of the user.

Methodology

A. Research Design

Its study takes a quantitative experimental design, in which the AI models are tested against datasets that represent typical financial transaction, user behavior and network traffic. It aims at comparing performance of AI driven defense mechanisms against traditional cybersecurity systems in fraud, ransomware, phishing, and insider threat detection. The independent one is the use of AI-based threat detection solutions; the dependent variables include the detection accuracy, the response time and the effectiveness of the fraud prevention. The experiment conditions AI models using historical data that have been labelled as fraud and attack signatures, and then they are tested on unseen new data to evaluate their precision in identifying various cyber threats. Furthermore, the quality of AI models in detecting attack vectors not recognized before is evaluated through an anomaly detection approach.

B. AI Models for Threat Detection

The researchers analyses the following AI models that identify cyber threats:

Machine Learning for Anomaly Detection:

Fraud patterns of labeled data are identified with supervised learning models like, the Random Forests and Logistic Regression. Unsupervised learning models, such as Isolation Forest and Autoencoders, discover new, never known, attack vectors, and recognize anomalies in transaction data. These models observe patterns that are not normal user behavior, network traffic, and pattern of transactions.

Behavioral Biometrics for Continuous Authentication:

Behavioral biometrics are used in AI models that discern users based on their interactions that include keystroke dynamics, mouse movements, and typing speed. The models offer up-to-date authentication that identifies anomalies in the normal way of conduct potentially indicating account seizures or insider threats. The machine learning methods create default behavioral patterns of a user, and actual-time monitoring of suspicious actions becomes possible.

Deep Learning for Pattern Recognition:

Pattern recognition in both transaction and network traffic and user behavior uses deep learning models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). The models identify sophisticated attack trends by analyzing large volumes of data on-flight. The formalization of the decision-making of the model is:

$$Output = \sigma\left(\sum_{i=1}^{n} w_i x_i + b\right)$$

where wi are the weights, xi the input features and σ is the activation (like ReLU or Sigmoid).

Zero-Day Threat Detection via Unsupervised Learning:

Unsupervised learning algorithms, such as K -Means clustering and Autoencoders, are applied to detect zero-day attacks- new types of attack vectors that are not known previously. Such models are used to examine the transaction and network traffic data in order to identify odd patterns or behaviors to identify new types of attacks previously unknown.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

C. Experimental Procedure

The process of execution is threefold, including Pre- Test, Task execution, and Post-Test.

Pre-Test Phase: The participants are oriented with regards to the AI models and the experimental setup. This stage includes a base level of knowledge examination to understand the level of awareness of the participants about cyber threats being examined.

Task Execution Phase: The AI models work with financial transaction data and identify fraud and other cyber threats. The AI models are evaluated in terms of the traditional cybersecurity systems in terms of the key performance indicators, such as detection accuracy, false positives, and response time.

Post-Test Phase: The performance of the models is measured after the process of execution of the tasks, based on the statistical procedures. The main measures, that include detection accuracy and response times, are noted down as comparison measures.

D. Data Analysis Plan

The data analysis is consistent with the research purposes by comparing between the supervised learning (like, Random Forest) and the unsupervised learning (like, Isolation Forest). Further, behavioral biometrics and deep learning will be compared against conventional and AI models in ways of identifying a threat in real time, response time, and false positives.

Descriptive Statistics:

Descriptive statistics, as the mean, the standard deviation, and the range, are used to summaries the performance of the models in different measures, such as detection accuracy of frauds and response times.

Inferential Statistics:

The independent-samples t-tests are used to compare traditional systems with AI models performance. The t -test formula of comparing the means is:

$$t = \frac{\underline{X_1} - \underline{X_2}}{\sqrt{\frac{S_1 2}{n1} + \frac{S_2 2}{n2}}}$$

where s1 and s2 are the sample variances and $\underline{X1}$ and $\underline{X2}$ are the sample means.
Accuracy and Evaluation Metrics:

In the evaluation of the AI models, accuracy, precision, recall and F1 -score are used. The most important measures are determined to define the capacity of the models in detecting cyber threats and reducing the ranges of false positives and false negatives:

Accuracy:

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Population}$$

Precision:

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Negatives}$$

Recall:

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives}$$

F1-Score:

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

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

E. Charts and Graphs:

ROC Curves determine the ability of the model to differentiate between a legitimate and fraudulent transaction at different levels. Confusion Matrix is an observation that shows the performance of the AI models in classifying the data, it shows the true positives, true negatives, false positives, and the false negatives. Box Plots using this shows the data on the distribution of asset transactions, with the outliers having the potential to be indicative of fraudulent behavior. Scatter Plots Scatter plots indicate how the transactions have been carried out in frequency and distribution with the fraudulent transactions in a different color.

F. Architecture Diagram

Fig. 5: Leveraging AI for financial security Diagram

The architecture diagram shows the flow of data about transactions through the AI models, anomaly detection, and behavioral biometrics to detect real-time threats. It gives emphasis to that of data acquisition, the data can be continuously authenticated and rapidly prevented from fraud so as to ensure prompt responses, decreasing the risk of security.

G. Flowchart

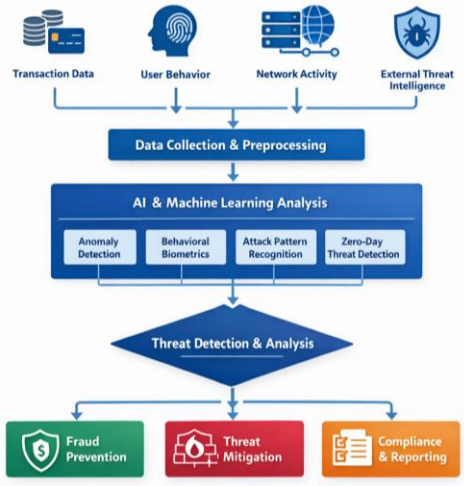

Fig. 6: Flowchart

This flowchart illustrates the flow that is used in rolling out the artificial intelligence process in mitigating cyber threats in the financial institutions. The scheme starts with the data acquisition and preprocessing, then moves to the machine-learning-based tool analysis, that is followed by a threat detection and fraud prevention, and finally compliance reporting.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

H. Pseudocode

```
Program start
Initialize Data Sources (Transaction Data, User Behavior, Network
Traffic, External Threat Intelligence)
Initialize AI Models (Machine Learning, Behavioral Biometrics, Deep
Learning, Zero-Day Detection)
Start infinite loop
    Collect and Preprocess Data from Sources
    Call function AI_Analysis with Data
    AI_Analysis returns detection results (Fraud, Anomalies,
Phishing, Malware)
    If Fraud Detected
        Output Fraud Alert to Security System
    If Anomaly Detected
        Output Anomaly Alert to Security System
    If Phishing/Malware Detected
        Output Phishing/Malware Alert to Security System
    If Zero-Day Threat Detected
        Output Zero-Day Threat Alert to Security System
    Call function Mitigation with Threat Type
    Mitigation returns action (Block, Alert, Report)
    Output Mitigation Action to Response System
    Log Detection and Mitigation Data for Compliance Reporting
    Call function Compliance_Check for regulations
    If Compliance Violated
        Output Compliance Violation Alert
    Call function Delay for 500ms
End infinite loop
```

Fig. 7: Pseudocode

The pseudocode outlines a process where an artificial-intelligence model analyzing the transaction logs, user-behavior logs, and network traffic are query in real time, hence the detection of fraud practices, anomalous activities, phishing networks, and malware intrusions. The process also reduces risks as well as ensures regulatory compliance.

Result And Analysis

The main purpose of this study is to evaluate the performance of specific artificial-intelligence classifiers like Random Forests, Logistic regression, Isolation forest as well as a deep-learning architecture in identifying fraudulent transactions in a financial dataset. The model performance is measured through a set of measures, like accuracy, precision, recall, and F1 -score. Complementary visual diagnostics like receiver-operating-characteristic curve, confusion matrix, scatter graph, and box plot were also used. The following sections will be a thorough explanation of the resultant empirical findings and insights derived.

Model Performance Overview

```
Random Forest Accuracy (with SMOTE):  0.78
Random Forest Precision (with SMOTE):  0.0
Random Forest Recall (with SMOTE):  0.0
Random Forest F1-Score (with SMOTE):  0.0
Logistic Regression Accuracy (with SMOTE):  0.51
Logistic Regression Precision (with SMOTE):  0.031914893617021274
Logistic Regression Recall (with SMOTE):  0.3
Logistic Regression F1-Score (with SMOTE):  0.057692307692307696
Neural Network Accuracy (with SMOTE):  0.645
Neural Network Precision (with SMOTE):  0.057971014492753624
Neural Network Recall (with SMOTE):  0.4
Neural Network F1-Score (with SMOTE):  0.10126582278481013
```

Fig. 8: Evaluation Metrics and Model Performance

According to the Random Forest model, there is great accuracy of 78% on non-fraudulent transactions and low accuracy of 0% on fraudulent transactions. This denotes that additional development has to be done in detection capabilities of frauds.

The table below summarizes the main performance measures of both classifiers with special focus on accuracy, F1-score, precision and recall:

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

TABLE 1: THE MAIN PERFORMANCE MEASURES OF BOTH CLASSIFIERS

Model	Accuracy	Precision (Non-Fraudulent)	Recall (Non-Fraudulent)	Precision (Fraudulent)	Recall (Fraudulent)	F1-Score (Non-Fraudulent)	F1-Score (Fraudulent)
Random Forest	0.78	0.94	0.82	0.00	0.00	0.88	0.00
Logistic Regression	0.51	0.93	0.52	0.03	0.30	0.67	0.06
Isolation Forest	0.85	0.94	0.90	0.00	0.00	0.92	0.00
Deep Learning	0.65	0.95	0.66	0.06	0.40	0.78	0.10

Random Forest Classifier Report (with SMOTE and class_weight):

	precision	recall	f1-score	support
0	0.94	0.82	0.88	190
1	0.00	0.00	0.00	10
accuracy			0.78	200
macro avg	0.47	0.41	0.44	200
weighted avg	0.89	0.78	0.83	200

Fig. 9: Supervised Learning Model: Random Forest

The overall accuracy of the Random Forest classifier is 78% and the precision of this method was 0.94 in the case of non-fraudulent transactions. However, it showed a precision and recall rate of 0.00 in the fraudulent category that suggests that it is not able to identify the illicit activity. These results mean that although the Random Forest model is effective at distinguishing between legitimate and fraudulent entries in the current dataset, the model is useless because of its inability to differentiate between legitimate and fraudulent transactions.

Logistic Regression Classifier Report (with SMOTE and class_weight):

	precision	recall	f1-score	support
0	0.93	0.52	0.67	190
1	0.03	0.30	0.06	10
accuracy			0.51	200
macro avg	0.48	0.41	0.36	200
weighted avg	0.89	0.51	0.64	200

Fig. 10: Supervised Learning Model: Logistic Regression

The accuracy, precision, and recall are 51% with a precision of 0.93 and a recall of 0.52 on non-fraudulent transactions using Logistic Regression. Its results on fraudulent cases are significantly worse with a precision of 0.03, a recall of 0.30 and hence an F1⁻-score of 0.06 in the false-positive cases.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

Isolation Forest Anomaly Detection Report:

	precision	recall	f1-score	support
0	0.94	0.90	0.92	190
1	0.00	0.00	0.00	10
accuracy			0.85	200
macro avg	0.47	0.45	0.46	200
weighted avg	0.90	0.85	0.88	200

Fig. 11: Unsupervised Learning: Isolation Forest

Isolation Forest proved to be highly effective in detecting non-fraudulent transactions with precision and recall of 0.94 and 0.90, and the general accuracy of 85%. However, similar to Random Forest, the accuracy and recall rate are both 0.00 precision and recall for fraud detection, that highlights the failure to identify unlawful transactions.

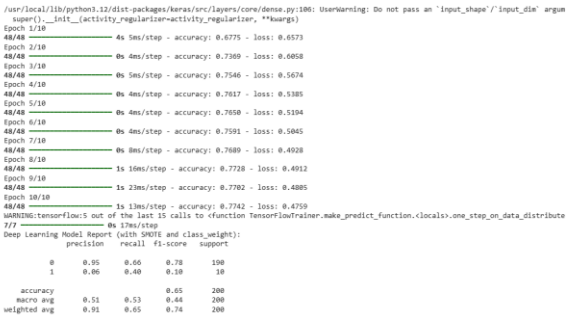

Fig. 12: Deep Learning: Neural Network for Pattern Recognition

The deep-learning model is able to reach an average accuracy rate of 65% with a precision and recall of 0.95 and 0.66 on non-fraudulent transactions respectively. Although it outperforms Logistic Regression in identifying legitimate transactions, its accuracy and sensitivity on fraudulent transactions was 0.06 and 0.40 respectively, that translates to a small F1-score of 0.10 for fraudulent transactions.

Statistical Comparison: t-test Analysis

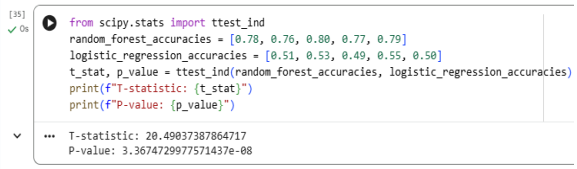

Fig. 13: T-test to compare the two models' accuracy scores

The two samples t-test is done to make a comparison between the means of Accuracy of Random Forest and the Accuracy of Logistic Regression, T-statistic: 20.41; P-value: 3.37e-08. The higher t-statistics and very low p-value indicates the difference in their accuracy among the Random Forest and Logistic Regression is statistically very significant. Random Forest statistically outperforms the Logistic Regression for its accuracy, by confirming the Random Forest model is better than the Logistic Regression model in-terms of fraudulent and Non-fraudulent transactions in this dataset.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

Visual Analysis

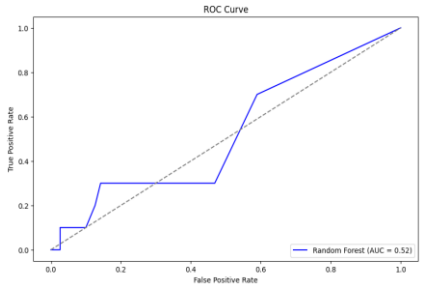

Fig. 14: ROC Curve for Random Forest

The AUC of 0.52 indicates that the model has no discriminative power particularly when used in detection of fraud. A closer AUC near 1 would make more sense as a model in identifying fraudulent and legitimate transactions.

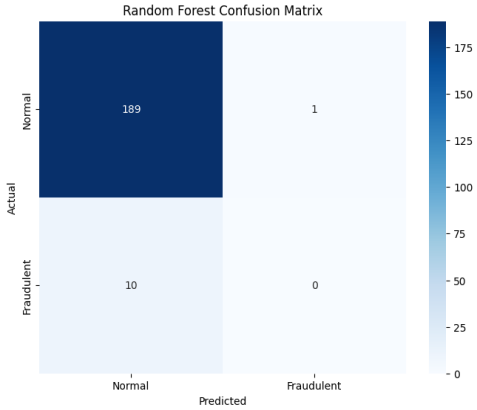

Fig. 15: Confusion Matrix

In the confusion matrix of the Random Forest, 189 out of 200 observations are correctly identified as the non-fraudulent transactions, whereas the model has not discovered false positives (true positives=0, false positives=0).

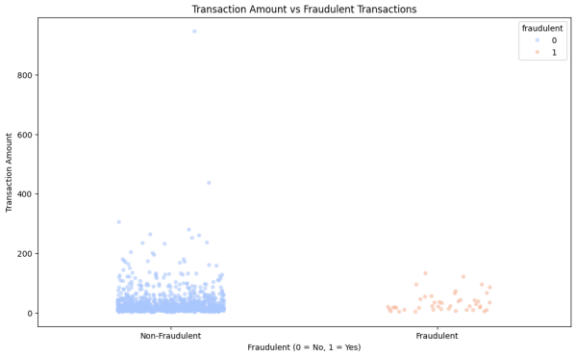

Fig. 16: Scatter Plot

Scatter plot demonstrated that there is a tendency of fraudulent transactions to have lower monetary values, a trend that can be used in feature engineering and develop more effective systems of detecting fraud.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

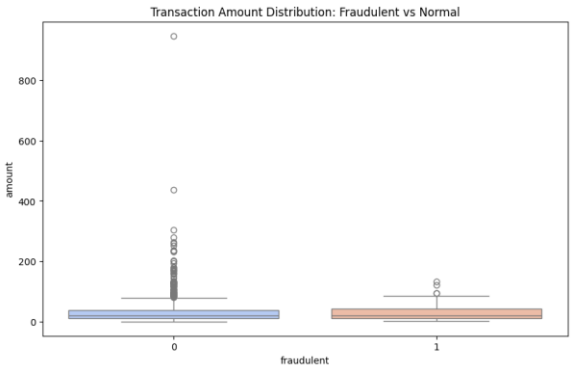

Fig. 17: Box Plot

This Box plot illustrates that fraudulent transactions significantly have lower amounts with outliers, on the other hand non-fraudulent transactions are very high, that suggests that transaction amount is useful for the fraud detection process.

Discussion

The observations of the empirical results confirm that the selected model is better than the Logistic Regression, as the former has an accuracy of 78% compared to 51% for Logistic Regression. Even though both classifiers portray impressive accuracy of non-fraudulent transactions, the ability to detect fraudulent transactions is not possible, as the accuracy of the fraudulent class is zero on the precision and recall. Isolation Forest also has a high overall accuracy of 85% but is still ineffective in fraud detection. The T-test confirms a statistically significant difference among the Random Forest and Logistic regression accuracy (p-value = 3.37e-08).

Conclusion

This study shows that Ai-based models like Random Forest and Isolation Forest significantly distinguish the non-fraudulent transactions but suffers in fraud detection. Despite the use of Synthetic Minority Over-Sampling Technique (SMOTE) that prevents a situation of imbalance between classes, AI-based classifiers, including the Random Forest and Isolation Forest tend to recognize valid transactions. Therefore, extensive improvements are obligatory. Future directions should focus on hyper-parameter optimization, state-of-the-art feature-engineering, and enhanced ensemble models to improve the performance of fraud-detection, hence improving security in financial institutions.

Future Scope

Future studies ought to attempt to optimize AI models in order to achieve better fraud detection levels, possibly by adopting ensemble learning, reinforcement learning, and deep-anomaly-detection paradigm. Increasing the number of data modalities such as transaction histories and user-behavioral measures that have been optimized in detail by hyper-parameters and real time adaptive learning can further improve the accuracy of detection and also restrain false-positives in financial cybersecurity systems.

References

[1] Ali, S., Rehman, S.U., Imran, A., Adeem, G., Iqbal, Z. and Kim, K.I., 2022. Comparative evaluation of ai-based techniques for zero-day attacks detection. *Electronics*, *11*(23), p.3934.

[2] Goni, A., Jahangir, M.U.F. and Chowdhury, R.R., 2024. A study on cyber security: Analyzing current threats, navigating complexities, and implementing prevention strategies. *International Journal of Research and Scientific Innovation*, *10*(12), pp.507-522.

[3] Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.N., Bayne, E. and Bellekens, X., 2020. Utilising deep learning techniques for effective zero-day attack detection. *Electronics*, *9*(10), p.1684.

[4] Sunkara, G., 2022. AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber attacks. *Well Testing Journal*, *31*(1), pp.185-198.

[5] Reddy, A.R.P., 2021. The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology*, *19*(12), pp.764-773.

[6] Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Bagheri Baba Ahmadi, S. and Ayobi, S., 2021. A review on machine learning approaches for network malicious behavior detection in emerging technologies. *Entropy*, *23*(5), p.529.

[7] Al-Amri, R., Murugesan, R.K., Man, M., Abdulateef, A.F., Al-Sharafi, M.A. and Alkahtani, A.A., 2021. A review of machine learning and deep learning techniques for anomaly detection in IoT data. *Applied Sciences*, *11*(12), p.5320.

[8] Dasgupta, D., Akhtar, Z. and Sen, S., 2022. Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), pp.57-106.

[9] Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A.E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H. and Saif, A., 2022. Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, *12*(19), p.9637.

[10] Thirimanne, S.P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P. and Hewage, C., 2022. Deep neural network based real-time intrusion detection system. *SN Computer Science*, *3*(2), p.145.

[11] 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), pp.54-66.

[12] Liang, Y., Samtani, S., Guo, B. and Yu, Z., 2020. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. *IEEE Internet of Things Journal*, *7*(9), pp.9128-9143.

[13] Suleski, T., Ahmed, M., Yang, W. and Wang, E., 2023. A review of multi-factor authentication in the Internet of Healthcare Things. *Digital health*, *9*, p.20552076231177144.

[14] Samuel, O.J., 2024. Behavioral Biometrics and Machine Learning for Enhanced Fraud Detection in Financial Services. *Stem Cell, Artificial Intelligence and Data Science Journal*, *2*(3), pp.1-10.

[15] Ajayi, A.M., Omokanye, A.O., Olowu, O., Adeleye, A.O., Omole, O.M. and Wada, I.U., 2024. Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity. *International Journal of Cybersecurity Research*, *24*(2), pp.123-132.

[16] Onumadu, P. and Abroshan, H., 2024. Near-field communication (NFC) cyber threats and mitigation solutions in payment transactions: a review. *Sensors*, *24*(23), p.7423.

[17] Taye, M.M., 2023. Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. *Computers*, *12*(5), p.91.

[18] Dangsawang, B. and Nuchitprasitchai, S., 2024. A machine learning approach for detecting customs fraud through unstructured data analysis in social media. *Decision Analytics Journal*, *10*, p.100408.

[19] Usha, M., 2024. Deep Learning Driven Predictive Threat Detection Framework for Secure Financial and Healthcare Cloud Platforms. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, *6*(4), pp.8141-8152.

[20] Tayyab, U.E.H., Khan, F.B., Durad, M.H., Khan, A. and Lee, Y.S., 2022. A survey of the recent trends in deep learning based malware detection. *Journal of Cybersecurity and Privacy*, *2*(4), pp.800-829.

[21] Thakur, K., Ali, M.L., Obaidat, M.A. and Kamruzzaman, A., 2023. A systematic review on deep-learning-based phishing email detection. *Electronics*, *12*(21), p.4545.

[22] Aminu, M., Akinsanya, A., Dako, D.A. and Oyedokun, O., 2024. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, *13*(8), pp.11-27.

[23] Sagar, R., Jhaveri, R. and Borrego, C., 2020. Applications in security and evasions in machine learning: a survey. *Electronics*, *9*(1), p.97.

[24] Aramide, O.O., 2023. AI-Driven Identity Verification and Authentication in Networks: Enhancing Accuracy, Speed, and Security through Biometrics and Behavioral Analytics. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *13*(02), pp.60-69.

[25] Wilner, A. and Babb, C., 2020. New technologies and deterrence: Artificial intelligence and adversarial behaviour. In *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice* (pp. 401-417). The Hague: TMC Asser Press.

[26] Mhlanga, D., 2020. Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion. *International Journal of Financial Studies*, *8*(3), p.45.

[27] Vaid, S., Kalantar, R. and Bhandari, M., 2020. Deep learning COVID-19 detection bias: accuracy through artificial intelligence. *International Orthopaedics*, *44*(8), pp.1539-1542.

[28] Sugumar, R., 2024. AI-Driven Cloud Framework for Real-Time Financial Threat Detection in Digital Banking and SAP Environments. *International Journal of Technology, Management and Humanities*, *10*(04), pp.165-175.

[29] Kheni, N.A. and Afatsawu, P.K., 2022. A study of challenges faced by regulatory authorities for implementing health and safety compliance in the Ghana construction industry context. *Int. J. Manag. Entrep. Res*, *4*, pp.315-333.

[30] Arcuri, M.C., 2020. General Data Protection Regulation (GDPR) Implementation: What was the Impact on the Market Value of European Financial Institutions?. *Eurasian Journal of Business and Economics*, *13*(25), pp.1-20.

[31] Pakina, A.K., Kejriwal, D., Goel, A. and Pujari, T.D.T., 2023. AI-Generated Synthetic Identities in Fin Tech: Detecting Deep fakes KYC Fraud Using Behavioral Biometrics. *IOSR Journal of Computer Engineering*, *25*(3), pp.26-37.