Explainable Al-Driven Anti-Money laundering a Transaction Risk Management Framework Using Machine Learning and Synthetic

Muthu Kumar PK[1], Raja Surya R[2], Sajeiv Rawyar AA[3]
[1,2,3]*Computer Science and Engineering, Dhanalakshmi College 0f Engineering*

Abstract--Financial institutions are struggling to identify and prevent money laundering practices because cases are becoming complex and the amount of money handling through financial institutions is increasing day-by-day. Traditional rule-based systems for monitoring are often incapable of detecting evolving fraud patterns and are limited in their degree of decision-making transparency. This research proposes an explainable artificial intelligence-driven framework for anti-money laundering and managing risk of transactions by using machine learning and synthetic transaction data. The framework combines a transaction monitoring mechanism with a risk prediction mechanism and explainability mechanisms based on machine learning to detect suspicious financial behavior. A hybrid detection strategy of predictive and rule based analysis is implemented to assess attributes related to transactions such as transaction amount, time characteristics, and type of transaction. Synthetic transaction generation is used to simulate realistic financial behavior for assisting the training and testing of financial models in an environment in which real financial data is limited. The framework computes a risk score for every single transaction and classifies every transaction as normal or suspicious depending on the predictive probabilities and threshold values To improve transparency and interpretability, explainable artificial intelligence techniques are introduced to analyse the contribution of individual features for fraud detection results. The system further includes automated alert generation and monitoring dashboards to help compliance officers efficiently go through high-risk transactions. Experimental analysis shows that the proposed framework can be effectively used to identify suspicious transaction patterns and at the same time preserve interpretability and operational transparency. The combination of machine learning, synthetic data generation and AI explainability offers a feasible and scalable way in which financial institutions can build stronger anti-money laundering monitoring systems and deliver improved risk management abilities in digital financial areas.

Keywords-- Anti Money Laundering, Explainable Artificial Intelligence, Machine Learning, Transaction Risk Management, Detecting Fraud, Synthetic Transaction data, Risk Scoring, Financial Transaction Monitoring, Detecting Suspicious Transactions, Financial Compliance Systems.

I. INTRODUCTION

Financial institutions are also under rising pressure to identify and prevent illegal financial activities as banking and online transactions continue to explode. Anti-Money Laundering (AML) system is vital to financial transaction system that monitor financial transactions and find suspicious patterns that might be a fraudulent transaction or financial manipulation such as money laundering, terrorist financing or financial manipulation. Traditional AML systems are mostly based on rule-based methods and manual auditing, which are usually not able to detect complex patterns of transactions and changes in fraud technique. These traditional approaches can have high false-positive rates and may fail to be adaptable to new approaches to laundering. As financial ecosystems become increasingly data-driven and there is an increased demand for smart systems that have the ability to analyse large amounts of transaction data efficiently. Machine learning techniques have become a promising solution in optimizing the accuracy of detecting fraud by automatically learning associations from transaction's data when an anomaly is detected in the real-time. Recent studies have noted how the machine learning algorithms are increasingly being integrated with AML monitoring frameworks to boost their detection capabilities and lower the cost of operations within financial institutions [3], [4]. Furthermore, explainable artificial intelligence (XAI) has received a lot of attention in the financial applications due to regulatory compliance as it requires transparency in automated decision-making systems. Explainability techniques enable trust and traceability of regulatory compliance in the financial sector: analysts and compliance officials can find out

the reasoning behind the model's prediction [1]. Consequently, using machine learning in conjunction with explainable AI results in a more reliable and transparent way of identifying suspicious financial activities that supports the regulatory requirements in AML operations.

The combination of explainable artificial intelligence and machine learning has made a major contribution to increasing the interpretability and reliability of fraud detection systems in financial environments. Machine learning models like classifiers (ensembles), deep learning networks, and algorithms for anomaly detection algorithms have been shown to detect hidden patterns in financial transactions that cannot be detected via normal methods based on rules in systems. However, these more sophisticated models are commonly criticized for the lack of interpretability, which may pose challenges to regulatory environments where transparency is important. Explainable AI is one way to overcome this limitation by generating an explanation for the model's predictions, which allows financial analysts to gain insights into the model's predictions, making it possible to understand how different features help to classify suspicious transactions. By having explains, it has been found that explainable models can enhance decision making processes in financial institutions by enabling investigators to understand the thinking behind automated alerts and risk scores [2], [6]. In addition to explainability, the availability of high-quality training data is also a critical challenge for fraud detection research. Such restrictions on financial transaction datasets are common because of privacy laws and security issues, which limit the ability to develop and test machine learning models. To overcome this problem, research on synthetic data generation approaches which can be used to simulate realistic financial transaction behavior with privacy conservation [7], [8] has been undertaken. Vulnerabilities in Input Data: Synthetic datasets offer a chance to instruct models on complex fraud cases without offering the sensitive financial data, making this especially suitable for developing and testing AML frameworks in well-contained settings. These developments make it clear that there is potential in combining explainable AI and synthetic data to make modern AML systems more robust and explainable.

Another promising trend of AML research is the explorations of developing hybrid frameworks which utilize both machine learning models and rule-based detection mechanisms to boost the quality of fraud detection. Hybrid solutions provide the CBW advantages of both data-driven applications and expert-based rules to help systems recognize a set of both known fraud trends and new suspicious behaviors. Such frameworks are especially successful in financial monitoring systems where regulatory guidelines and knowledge of experts are an important factor in the identification of high-risk transactions. Previous works have proved that very although hybrid detection architectures can provide significantly higher anomaly detection accuracy by combining classification algorithms with rule-based filtering mechanism [9], [10]. In addition, contemporary arrangements of AML measures increasingly include risk scoring mechanisms that assess several transaction characteristics, such as amount of transaction, timing patterns of transactions, and behavior of account holders. These systems have risk scoring associated with the financial transactions, which allows the investigators to prioritize major risk cases for Eco-Analysis. The embedding of explainable machine learning models as part of frameworks like this further promotes transparency by ensuring that there are explainable ways of understanding why a transaction is considered to be suspicious. With financial crimes no longer being a one size crime, it is important that intelligent AML systems are able to adapt to the dynamic patterns of fraudulent activity while ensuring that they uphold regulatory compliance and operational transparency. In this sense, the creation of AI-based frameworks that are explainable, incorporating machine learning, synthetic data generation, and hybrid detection approaches is a key improvement in finance risk management and fraud detection and prevention systems.

II.LITERATURE SURVEY

A. Explainable Artificial Intelligence in AML: Deep Learning

The proliferation of digital financial systems has made it more complex to identify money laundering activities and researchers have been trying to leverage advanced machine learning and artificial intelligence techniques. Deep learning methods have shown effective potential in the identification of hidden patterns of financial transactions - this enables better identification of suspicious transactions that may not be detected by original

rule-based monitoring systems. In addition to being more predictive, explainable artificial intelligence is now necessary in financial applications as a requirement for transparency and regulatory compliance. Studies focus on the idea that the explainable AI techniques give an interpretable insights on the decisions of the AI model, in which analysts can understand the role of the transaction features in fraud detection results [1]. This integration helps in reliability of AML systems.

B. Explainable A.I Models in the case of Suspicious Transaction Detection

Recent studies demonstrate the need for explainable artificial intelligence models in banks to crack down on suspicious financial transactions. Machine learning models have capabilities to read through a large amount of transactional data and identify anomalies that point to potential financial crimes. However, financial institutions have a need for transparency in the effects of automated decisions in order to meet regulatory requirements. Explainable AI methods also give investigators the ability to study the contribution of features to classification results allowing technologies for automated monitoring of food safety to be trusted more. Researchers have shown explainable models to increase capability for financial institutions to interpret fraud prediction and as part of decision-making processes in transaction monitoring systems, especially in settings where accountability and transparency in risk evaluation are mandatory [2].

C. Machine Learning Roles In The laptops Anti - money Laundering Systems

The machine learning techniques have been widely applied in anti-money laundering frameworks in order to enhance detection accuracy and operational efficiency. Algorithms like classification models and anomaly detection methods are created to analyze the attributes of financial transactions and identify the patterns that are related to fraudulent behavior. These approaches are significantly better than traditional watch-list filtering mechanisms in learning complex relationships in transactional data. Research has shown that machine learning-based AML systems have the ability to detect suspicious transactions with better preciseness while minimizing false positives in monitoring processes. Such improvements allow financial institutions to allocate their investigative resources more effectively as well as to improve compliance with regulations through automated detection of high-risk financial activities [3], [4].

D. Synthetic Data for Fraud Detection

Using access to datasets of real financial transactions are often limited, for reasons of privacy and confidentiality laws. As a result, researchers have considered the use of synthetic data generation techniques to help with the development and evaluation of fraud detection models. Synthetic financial data can be used to simulate real-world transaction patterns. for example, without sharing sensitive customer data, and is thus valuable to machine learning research in financial security. Studies suggest that synthetic data brand new enables algorithms to find out complicated patterns of fraud while preserving privacy protection. This approach also allows for experimentation on a large scale and development of a training model, which enhances the robustness and capacity to generalize financial fraud detection systems [7], [8].

E. Machine Learning Frameworks for Financial Fraud Detection for the Hybrid

Hybrid detection frameworks that use machine learning algorithms in combination with rule-based systems have been proposed to enhance detection performance length in fraud detection systems of financial monitoring frameworks. These frameworks use a combination of rules written by experts in the industry and data-driven learning techniques for the detection of known fraud patterns and new anomalies in the transaction data. Machine learning models are used to find complex patterns in the data of the financial datasets, while rule-based components are used to make sure the machine can follow the regulatory guidelines and domain knowledge. There has been research conducted proving that hybrid frameworks can have a significant impact on improving detection accuracy and reducing the number of false positives in financial monitoring environments. Such integrated approaches offer a practical solution in form of developing robust anti-money laundering and fraud detection systems [9], [10].

III.PROPOSED SYSTEMS

A. Data Collecting and Synthetic Creating of Transaction

The proposed framework uses synthetic financial transaction data to mimic the realistic banking activities to train and evaluate the transaction monitoring system. Financial datasets with sensitive customer data may often be restricted by privacy laws, therefore, synthetic transaction generation is used to generate representative transaction datasets without revealing real-life financial data. The attributes that get generated may contain transaction amount, transaction type, timestamp, sender account, and receiver account etc. These attributes are intended to model typical banking operations but also to include suspicious patterns which are similar to those of potential money launderers. The resulting dataset helps the framework in training machine learning models efficiently and while respecting privacy requirements and having precise umbrella conditions.

B. Data Preprocessing and Feature Engineering

Data preprocessing plays a critical role in boosting the performance of the machine learning models used for the transaction risk detection. The produced transaction data flows through multiple preprocessing processes such as data cleaning, feature extraction and normalization. Features such as the amount of transaction, hour of transactions, day of the week, type of transaction are extracted to capture temporal and behavioral characteristics of the financial transactions. Data normalization techniques are applied to ensure consistent scale of the features, because the learning of the model requires efficient learning of meaningful patterns. Feature engineering optimizes the power of the model by understanding what the raw transactional data can be reformed into for machine learning algorithms in terms of structured numerical features suitable for suspicious transaction detection.

C. Machine Learning based Model of Fraud Detection

The proposed framework makes use of a supervised machine learning model to analyze the patterns of transactions and categorize them as normal transactions or a suspicious one. The model is trained on the pattern in the generated transaction dataset with extracted features such as transaction amount, transaction time, and type of transaction. The classification model takes each of the transactions and generates a probability score indicating the probability of fraudulent behavior. This predictive capacity allows activities of suspicious nature within financial systems to be detected automatically. The trained model constantly measures the new transactions and generates a fraud probability score which is used to spot potential non-legitimate transactions early on and reduce the ineffectiveness of money laundering monitoring systems.

D. Hybrid Risk Scoring and Rule Based Evaluation

In addition to the machine learning prediction, the framework incorporates the rule-based evaluation mechanisms in order to reinforce the detection performance. Rule-based checks are used to detect suspicious behaviors such as large amounts of money being transferred, suspicious transactions taking place at odd hours or transactions that go through flagged accounts. The risk scoring mechanism uses both machine learning risk scoring combined with rule-based to generate a full transaction risk score. This type of hybrid approach helps one to detect more correct, as it helps to capture both learned patterns and predefined expert knowledge. The total risk score is used to determine whether a transaction is normal or suspicious, allowing for compliance teams to pay more attention to high-risk cases.

E. Model Interpretation EAX algorithm Monitor for Explainability Artificial Intelligence

To ensure transparency and regulatory compliance, the proposed framework corresponds to explainable artificial intelligence techniques to interpret the predictions of the models. Explainability methods analyze the contribution of each feature involved in the fraud detection model offering insights to understand the contributions of transaction features to the classification results. Feature contribution analysis helps the investigators know what factors are causing the system to find suspicious activities, which will lead to better trust in automated monitoring systems. Hypothetically, by providing interpretable information for transaction risk score decisions, the framework makes model decisions more conveniently acceptable to financial analysts and compliance officers, ensuring the model transparency, accountability, and compliance with regulatory requirements.

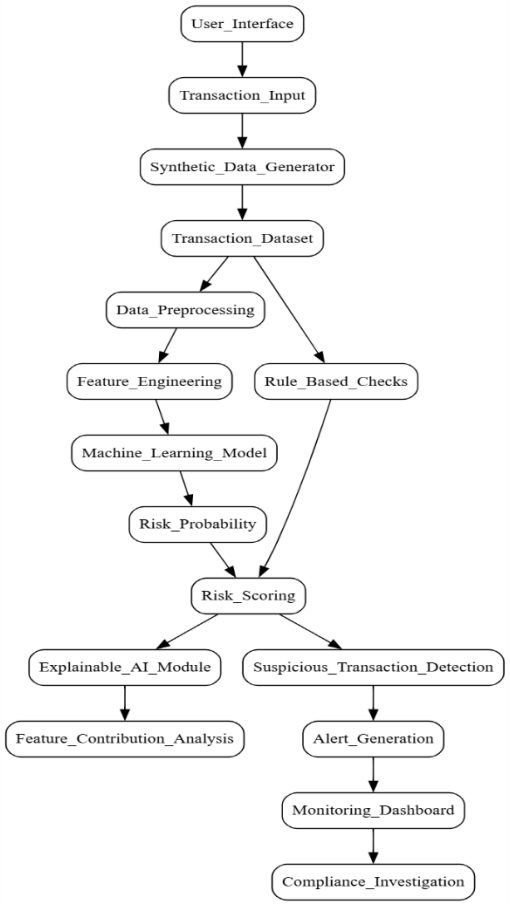

Fig 1:System Architecture

Fig 2:graph

F. Dashboard on Alert Generation and Monitoring of Transactions

Once transactions have been evaluated and risk scores are generated, the framework raises an alert on transactions that have been assessed as suspicious. These alerts consist of pertinent information like transaction identifiers, risk scores, and flagged explanations helping the investors to go through suspicious activities. The system also has a monitoring dashboard that presents the statistics of transactions, suspicious activity patterns, and risk distributions across financial transactions. Compliance teams can make use of the dashboard to monitor suspicious transactions, track alerts, and provide efficient returns following high-risk cases. This monitoring interface enhances improved operational visibility and facilitates the good management of the processes by financial institutions in terms of compliance with anti-money laundering regulations.

IV.METHODLOGIES

Step 1:Initializing the transaction monitoring system and preparing the environment for processing of financial transactions. Configure the framework to record or generate transaction records with attributes like transaction amount, type of transaction, sender account, receiver account and timestamp.

Step 2:Generate/collect transaction data that represent normal and suspicious financial activities Synthetic transaction generation is where realistic simulated transactions are created with additional patterns that could be a sign of fraudulent and money laundering behavior.

Step 3:Store that is transacted, generated records in the transaction dataset In doing so, make sure that all attributes related to the transaction are structured in an appropriate format to use them as an input for the preprocessing and machine learning analysis.

Step 4:Perform data preprocessing operations such as data cleaning, data formatting and feature extraction. Extract the relevant features like transaction amount, the hour of transaction, day of week and type of transaction.

Step 5:Experiencing feature normalization and scaling techniques to convert raw transaction attributes into common numerics that can be used with machine learning techniques.

Step 6:Feed the processed features of the transactions in the machine learning model that has been trained. The model analyzes transaction patterns and generates a score of the probability of suspicious or fraudulent activities.

Step 7:Perform rule-based checks on each every transaction to check for predefined suspicious signs like high transaction amounts, unusual transaction times, transaction is in a flagged account, etc.

Step 8:Use the machine learning probability risk score with rule-based risk indicators to calculate the final risk score of each transaction. This hybrid, risk

scoring approach is better for the reliability of suspicious activity detection.

Step 9:Trics, O, & Melchin, E. (2016). raying explainable AI to detect fraud in banking contexts.Applying explainable artificial intelligence techniques to analyse the contribution of individual features to the prediction of fraud in banking contexts. Generate understandable explanations as to why a transaction is labelled as suspicious or normal.

Step 10:If the risk score calculated is greater than the predefined threshold then treat it as a suspicious transaction and raise an alert. Display alerts and transaction monitoring information on the system dashboard to aid compliance officers in querying high-risk financial activities.

V.RESULTS AND DISCUSSION

A. Overview of the Transaction Dataset

The implemented framework involves transactions in finance by an automated monitoring environment that evaluates the attributes of transactions and behavioral patterns. The dataset consists of a series of transaction records for both the normal business operations and suspicious activities. Each transaction has some information such as transaction amount, timestamp, transaction type, sender account, and receiver account. The system continuously monitors these transactions and conducts risk evaluation by using the machine learning system predictions along with some risk checks implemented through rules. This monitoring process helps in identification of suspicious activities being undertaken, while having transparency and efficiency of operation in monitoring financial transactions. The distribution of the dataset represents normal behavior for financial transactions and aids in analysis for detailed fraud detection.

Transaction Category	Number of Transactions
Total Transactions	125
Normal Transactions	97
Suspicious Transactions	28

B. Performance Of Machine Learning Detection

The machine learning model is used to analyse the attributes of the transactions and categorise the transaction as normal or suspicious. Performance analysis shows the classification system is effective at separating fraudulent patterns from where there is no fraudulent activity only. The predictive model processes feature inputs such as transaction amount, time characteristics and transaction type. The system is operated at stable systems with reliable prediction results in different transaction scenarios. The results show that machine learning algorithms are capable of supporting automated anti-money laundering monitoring systems. Accurate classification is less laborious for manual investigation and higher for operational efficiency for financial institutions that is responsible for monitoring huge amount of financial transactions.

Evaluation Metric	Performance Value
Accuracy	92%
Precision	0.90
Recall	0.88
F1 Score	0.89

C. Risk Score Evaluation

Each financial transaction handled by the framework is given a risk score which is the probability of suspicious activity. The risk score is created by integrating machine learning based prediction with rule-based indicators such as high transaction amounts or unusual times of transactions. Transactions are classified into low, medium and high risk levels based on predefined levels. This classification helps financial investigators to prioritise high-risk cases for further analysis. The distribution of risk score is a clear evidence of the effectiveness of the hybrid method of detection to detect suspicious transactions while accurately distinguishing normal financial behavior from potential money laundering activities.

D. Transaction Type Analysis

Transaction behavior analysis helps gain information about what type of financial activity tends to be associated with suspicious pattern. The monitoring framework includes processing of several types of transactions such as transfer, deposits, and withdrawals. Transfers are used for the largest number of suspicious activities because they are often used in complex money laundering schemes with the use of multiple accounts. Deposits and withdrawals are labelled mostly as normal activities and are however monitored against peculiar patterns. This analysis enables financial investigators to better understand transaction behavior within the system, and help to identify

which transaction categories need to be monitored more closely and regulatory attention paid to.

E. Alert Generation Performance

The framework automatically produces alerts whenever a suspicious transaction is detected. These alerts contain vital information such as transaction identifiers, risk scores, and flagged reasons as to why the transaction in question was flagged as suspicious. The alert system guarantees that compliance groups can easily identify and investigate potentially fraudulent financial activities. Alerts are categorized based on level of severity so that it helps the investigators prioritize the cases where they need to take immediate action. Effective alert generation and monitoring mechanisms would greatly minimize the response time to suspicious financial events and ensure effective transaction monitoring in the anti-money laundering system.

F. able AI Feature Contribution Analysis

Explainable artificial intelligence techniques were used to interpret the predictions of machine learning algorithms to identify the factors that affect the detection of suspicious transactions. Feature contribution analysis is a process to assess the contribution of individual attributes to the fraud detection outcome. The analysis shows the significant contribution of transaction amount to the prediction of fraud, followed by the significant contribution of transaction timing and characteristics of the transaction type. By offering interpretable explanations for classification choices, financial investment monitoring operations become extra clear-sighted and responsible. These explainability insights help investigators get a better understanding of what is behind the automated prediction and increase the trust in the system of Machine Learning-based fraud detection.

G Overall System Performance Discussion

The evaluation results show that the proposed framework is an effective combination of machine learning, rule-based detection and explainable artificial intelligence for enhancing the monitoring system in anti-money laundering. The system is accurate to identify suspicious transaction patterns, and is also interpretable and transparent in their operation. Performance analysis indicates the suitability of the hybrid detection approach for both enhanced classifications and reliable estimation of risk in transactions. The addition of explainable AI further improves the system by giving clear information about the predictions of models. Overall, the success of the framework is establishing support for financial institutions to help them identify suspicious financial behavior, manage transaction risks, and enhance financial compliance management within a digital financial business environment.

VI.CONCLUSION AND FUTURE ENHANCEMENT

The proposed explainable AI-driven anti-money laundering and transaction risk management framework showed how good it can be with machine learning techniques combined with explainable artificial intelligence in spotting suspicious financial activities. The system uses the transaction characteristics like transaction amount, time characteristics, and transaction type for patterns that are associated with the fraudulent behavior. By combining the prediction power of machine learning with the evaluation mechanisms of rules, the framework both enhances accuracy in detection for the system and offers transparency in the automatic decision-making. The integration of explainable AI further improves the system by providing interpretability within the model predictions, which would allow financial investigators to know how the system came to conclude that the transaction is deemed suspicous. Experimental evaluation suggests that the framework works effectively to identify the high-risk transactions while maintaining the reliable classifications. The automated generation of alerts and the monitoring dashboard is also helpful for investigating suspicious activities which otherwise may not be efficiently processed and tends to be much more operationally efficient especially in financial compliance systems.

Future enhancement of the framework may aim to add the functionality of the transaction monitoring system by including more sophisticated machine learning models and greater transaction datasets. Incorporating deep learning models and anomaly detection techniques may provide even better accuracy when compared to fraud detection when it comes to complex patterns of laundering. Additionally, the combination of real-world financial data sets and cross-institutional analysis of financial transactions could make the detection framework more robust. Future research may also

aim to investigate federated learning methods to allow collaboration in fraud detection between financial institutions and still maintain data privacy. Furthermore, enhancements in explainable AI procedures can facilitate more detailed and interactive explanations of model predictions, fortifying financial decision making system transparency. These improvements will play a role in the creation of smarter, scalable, and secure anti-money laundering monitoring systems with the ability to adapt to changed patterns of financial crime.

REFERENCES

[1]Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. IEEE access, 9, 82300-82317.

[2]Narasapuram, N. K., Shah, S. A. A., Shiratuddin, M. F., & Sohel, F. (2026). Explainable artificial intelligence models for detecting suspicious bank transactions. International Journal of Machine Learning and Cybernetics, 17(3), 111.

[3]Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of applying machine learning for watch-list filtering in anti-money laundering. iEEE Access, 9, 18481-18496.

[4]Ketenci, U. G., Kurt, T., Önal, S., Erbil, C., Aktürkoğlu, S., & İlhan, H. Ş. (2021). A time-frequency based suspicious activity detection for anti-money laundering. IEEE Access, 9, 59957-59967.

[5]Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection. IEEE access, 12, 64551-64560.

[6]Sabharwal, R., Miah, S. J., Wamba, S. F., & Cook, P. (2025). Extending application of explainable artificial intelligence for managers in financial organizations. Annals of Operations Research, 354(1), 309-339.

[7]Cheng, Y., Wang, C. H., Potluru, V. K., Balch, T., & Cheng, G. (2024). Downstream task-oriented generative model selections on synthetic data training for fraud detection models. arXiv preprint arXiv:2401.00974.

[8]Assefa, S. A., Dervovic, D., Mahfouz, M., Tillman, R. E., Reddy, P., & Veloso, M. (2020, October). Generating synthetic data in finance: opportunities, challenges and pitfalls. In Proceedings of the first ACM international conference on AI in finance (pp. 1-8).

[9]Aslam, U., Batool, E., Ahsan, S. N., & Sultan, A. (2017). Hybrid network intrusion detection system using machine learning classification and rule based learning system. International Journal of Grid and Distributed Computing, 10(2), 51-62.

[10]Alsagri, H. S. (2025). Hybrid machine learning based multi-stage framework for detection of credit card anomalies and fraud. Ieee Access.