Journal of Information Systems Engineering and Management
2025, 10(32s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Global Banking Security: A Novel Approach Integrating Federated Learning and CNN-GRU for Effective Anti-Money Laundering Measures

Er. Arun Chaudhari[1*], Dr. Mandeep Kaur[2]

[1*] *Student, Computer Science and Engineering, CT University, Punjab, India. aronchaudhary06@gmail.com*
[2] *Lecturer, Computer Science and Engineering, CT University, Punjab, India. mandeep17209@ctuniversity.in*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Present-day banking sector analysis shows the growth of concern on AML in the face of sophisticated laundering practices by financial houses. Traditional means of detection in such cases seem to be out of the loop because of voluminous data in the system and dynamic nature of financial transactions. This research intends to boost global banking security through the implementation of Federated Learning (FL) with Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU) for an enhanced AML system. It caters to the necessity of privacy-preserving solutions, increasing the detection accuracy. This proposed method relies on FL so that sensitive financial data is decentralized; hence, the institutions are capable of collaborative learning of patterns in fraudulent activities without infringing upon their privacy. This has allowed the model to significantly improve anomalous transaction patterns detection, which was previously quite difficult due to the inability of CNNs in feature extraction to capture temporal dependencies. 98.7% of accuracy gains from this combination are very promising since hybrid models outperform conventional AML systems in efficiently processing large and complex datasets while eliminating false positives. This study shows how the innovative integration of FL, CNN, and GRU improves not only the detection capabilities but also ensures that stringent privacy regulations are met. Thus, the proposed method offers a scalable and effective solution for the global banking sector. It also surpasses traditional techniques in terms of security and efficiency in the battle against money laundering in the emerging financial scenario.

Keywords: Anti-Money Laundering (AML), Federated Learning, Privacy-Preserving, Intrusion Detection, Hybrid CNN-GRU Model

INTRODUCTION

Over the last few years, money laundering has turned into one of the most prevalent types of financial crimes in the entire world and has implications to the stability of financial institutions. The never-ending rise of financial activities, especially accompanied by sophisticated techniques used by the offenders, has led to the complicated nature of money laundering detection and prevention[1] [2]. There are typical methods in "AML": rule-based systems and manual analysis of bank transactions [3] as suspicious activities. However, these methods have some drawbacks. firstly, with the management of the large amount of data generated daily, and secondly, with the detection of subtle patterns in financial transactions. Due to modern development in the field of ML and DL, more efficient techniques are implemented that enhance the efficacy of identifying the fraudulent activities to a large extent. Despite this, methods such as decision trees, "SVM", and ensemble models, provides a promising means for detecting suspicious transactions [4]. However, these models have their drawbacks, including the inability to generalize results, concerns with data privacy, and worse the models are unable to handle issues of class imbalance that results into higher levels of false positives or negatives. To overcome these challenges, researchers have used complex methods like "CNN" and "RNN" [5] and many more for improving "AML" systems performance. Although holding great promise for enhancing detection accuracy, these methods have not without such drawbacks as overfitting, the need to obtain large amounts of labeled data, and data scalability. It is against this background that federated learning [6], a new concept in machine learning has been identified as a solution to these issues. Federated learning is a method which enables several institutions to train a model on a distributed data meanwhile; data privacy issues are considered[7] [8]. The application of this approach has emerged recently in the context of AML domain, as it allowed addressing the large distributed datasets and minimize privacy concerns [9].

In this work, a new approach to support AML prediction is presented, using federated learning with CNN-GRU hybrid models [10]. The strategy suggested here adopts Kaggle dataset, which consists of several types of the financial transaction's datasets, to train the model and it will efficiently predict a money laundering transaction. The proposed model had better performance by having high precision and recall that also eliminates the major problems such as class imbalance and false positive results. Using the "CNN" for feature extraction and the GRU for sequential analysis, here developed a robust model of AML detection with an accuracy of 98.7%, outperforming previous methods. Moreover, federated learning approach makes it possible to train the model across institutions while avoiding the compromise of the privacy of such financial data hence facilitate the detection of money laundering cases effectively. This research is useful to extend the existing literature in the field of AML by proposing a novel solution that is capable of overcoming the key challenges which relates to data privacy, data accuracy, and speed of detecting fraudulent financial transactions.

The contributions are as follows:

- The paper introduces federated learning, which helps financial institutions cooperate in the detection of money laundering without having access to sensitive data about customers. This way, privacy is preserved, and anti-money laundering (AML) detection is achieved in an effective manner.
- In this research, "CNN" and "GRU" are incorporated in order to provide an efficient feature extraction process and capturing temporal patterns in the transaction data. Thus, it aids in reduction of blunders in identifying money laundering employing a multiplicity of procedures.
- The model deals with the issue of evolving money laundering tactics through deep learning methods. It is able to identify subtle, complex patterns that the traditional models miss.
- The federated approach allows the model to scale multiple institutions without a central point and thus reduces inefficiency in such an operation; it lowers both computational and storage requirements and, at the same time, stays effective.

The order of the paper is as follows: Section 1 presents an introduction of all the work. Section 2 presents other related works. Section 3 overviews the issues with the current research. This paper used a methodology that is described in section 4. Section 5 gives the results of the study. Section 7 concludes the paper and pointer to the future works to be done.

RELATED WORKS

Vasudeva Murthy [11] work deals with AML compliance by Indian investment banks; his focus is on the processes of KYC and the training of employees. A study based on the data of 100 private and international bank employees suggests a general lack of awareness of and inadequate AML training are major barriers. Thus, the paper emphasizes rigorous programs and regulatory norms to enhance the overall compliance level. Reliance on survey data poses significant limitation since it cannot capture all the systemic AML weaknesses across the banking ecosystem.

Kandachamy [12]Study on the critical role AML rules play in the protection of the world financial system against illicit Case studies involving real-world experience emphasize that transparency, collaboration, and strong AML policies in addressing money laundering should be provided. Global cooperation and observance of the regulatory policy are important factors for an AML program to succeed. Lack of empirical verification limits its generalizability and applications for widespread use in diverse financial industries.

Sileshi [13] Evaluation of AML Measures adopted in Ethiopian Banks Using a descriptive statistics approach of an aggregate of 57 answers and interviews. Findings are gaps in AML compliance: communication of AML policies is poor third-party audits are absent-technology resources are minimal. While the study identifies critical areas of improvement, the absence of a national ID system and technical infrastructure further hinders AML efforts. The foremost limitation is the focus of the study on a single region, which restricts its applicability at broader levels.

Thommandru and Chakka [14] paper explores how blockchain technology can be the potential of AML compliances in peer-to-peer payments, KYC, and trade agreements. On the one hand, focusing on the financial burden banks face and the manipulation that occurs with AML policy, the study provides the framework to recalculate how compliance mechanisms are recalibrated. Blockchain appears as the promising tool to enhance the transparency and trust in a financial system. However, the study lacks strength because it is a paper-based approach that does not support its claims with real-time empirical validation or a pilot implementation.

Yi [15] analyzes the part that information technology plays in enhancing Anti-Money Laundering efforts in cross-border payment systems. Its focus is on the adoption of big data analytics, AI, and blockchain for AML compliance and improving regulatory efficiency. These technologies help financial institutions detect and prevent money laundering more efficiently. Although this paper addresses all the necessary issues, it does present some drawbacks, such as data privacy, technical compatibility, and security. The proposed countermeasures have practical solutions but underline the fact that the successful implementation depends on overcoming these barriers. A significant limitation of these advanced technologies is their resource-intensive nature in the process of deployment across the diversified financial landscapes.

M. Liu et al.[16] study AML enhancements in the context of Macau's gaming tourism destination, focusing on three major aspects: the adoption of technology, financial inclusion, and collaboration among various stakeholders. The study finds through the deployment of OLS multivariate regression analysis an increasing number of STRs positively correlated with domestic private-sector credit, while the investment in IT is statistically not important. The integration of the AML measures within both gaming and financial sectors contributes to positive outcomes concerning fraudulent activities. However, overreliance on data from STRs and less effectiveness of IT investment activities for AML suggest shortcomings.

Issah et al.[17] analyze the impact of AML regulations on banking sector stability in Africa using panel data for 51 countries over the period 2012-2019. The estimation results using a two-step Generalized Method of Moments (GMM) indicate that AML regulations improve financial stability regardless of the level of regulatory effectiveness. This research has a strong implication for AML compliance in the establishment and maintenance of a resilient banking system. One major limitation is that the study relied on macro-level data and failed to take into consideration country-specific or institutional factors that may influence AML implementation outcomes.

Gandhi et al. [18] investigate AI and, more specifically, machine learning (ML) in AML using data from the US Treasury's FinCEN. Various algorithms, including Random Forest, CNN, and Gradient Boosting, are used for tasks such as transaction type prediction. In this respect, the Random Forest classifier attained an accuracy of 99.99% in state prediction, proving that AI/ML can be effective in recognizing patterns of money laundering. While the results are promising, the reliance of the study on simulated datasets and the use of computationally expensive models do not make it scalable for real-world applications.

Maintaining international banking security with the help of Anti-Money Laundering Policies is still an important issue for the financial systems all over the world. Contemporary situations show that companies relocate from linear zeros and ones to modern tools such as big data, AI, blockchain, and ML. These technologies enhance the accuracy of detection results, facilitate monitoring in real time, and respond to further challenges of contemporary money laundering techniques. However, legacy techniques remain significant to address the fast pace and ensure that measurable and effective solutions revolve around the familiar concepts of KYC practices, regulatory compliance, and monitoring of transactions. Hindrances like data protection, size, compatibility, and the expensive nature of technology implementation are still felt today. Research done in this field is frequently underdeveloped with respect to application and evidence, and makes use of theoretical or restricted samples. As a result, further enhancements should focus on practical implementations, the combination of novel techniques with conventional approaches, the development of more extensive cooperation with other countries, and staff development programs for financial institutions. A sustainable and well-proportioned AML framework is paramount with regards to changing anti-money laundering threats.

PROBLEM STATEMENT

Maintaining international banking security with the help of Anti-Money Laundering Policies [19] is still an important issue for the financial systems all over the world. Contemporary situations show that companies relocate from linear zeros and ones to modern tools such as big data, AI, blockchain, and ML. These technologies enhance the accuracy of detection results, facilitate monitoring in real time, and respond to further challenges of contemporary money laundering techniques[20]. However, legacy techniques remain significant to address the fast pace and ensure that measurable and effective solutions revolve around the familiar concepts of KYC practices, regulatory compliance, and monitoring of transactions. Hindrances like data protection, size, compatibility, and the expensive nature of technology implementation are still felt today. Research done in this field is frequently underdeveloped with respect to application and evidence and makes use of theoretical or restricted samples. As a result, further enhancements should focus on practical implementations, the combination of novel techniques with conventional approaches, the development of more extensive cooperation with other countries, and staff development programs for financial institutions. A sustainable and well-proportioned AML framework is paramount with regards to changing anti-money laundering threats.

HYBRID FEDERATED LEARNING MODEL USING CNN-GRU FOR ANTI-MONEY LAUNDERING PREDICTION

The combination of CNN-GRU in the proposed hybrid federated learning improves the AML prediction while maintaining the customers' data confidentiality. Federated learning allows institutions to train models together without disclosing any information that is private. The workflow of CNN-GRU based approach in AML prediction is presented as Data Collection, along with the collection of the financial transaction records. In Data Pre-Processing stage, one has to work on the raw data in a way the data is ready for mining, this involves handling on missing values, anomalies and outliers. After data pre-processing for normalizing the data, the data flow is then subjected to the CNN-GRU model, which is a CNN-GRU hybrid neural network which comprises of both Convolutional Neural Networks (CNN) which is used to do feature extraction only and Gated Recurrent Units (GRU) used for temporal anomaly detection only. In light of privacy, the system implements Federated Learning that allows training a model in distributed nodes without transmitting raw data. This integration makes it possible to conduct safe, extensible analysis of the data without compromising the privacy of the users. Last, the Hybrid Fed-CNN-GRU model is used for predictions for AML with Performance Evaluation for metrics. The presented end-to-end process corresponds with modern issues in early and accurate detection of fraud in financial activities preserving confidentiality and possessing a high speed. Fig.1 represents the diagram for Anti-Money laundering prediction.

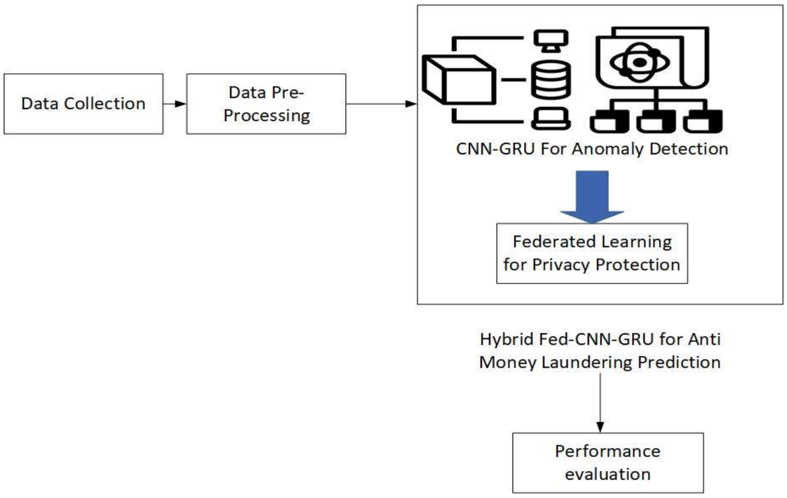
Data Collection
Data Pre-Processing
CNN-GRU For Anomaly Detection
Federated Learning for Privacy Protection
Hybrid Fed-CNN-GRU for Anti Money Laundering Prediction
Performance evaluation

Fig.1 block diagram of proposed CNN-GRU Method

4.1 Data Collection

Based on the existing AML literature, this research applies the Anti-Money Laundering Transaction Data (SAML-D) dataset [21]on the grounds of the identified limitations. The problem with the current traditional "AML" procedures is that they are slow, restrictive in data and access due to sensitivities around privacy without compromising quality and most importantly, there is a lack of mixed bag/high quality and diverse data. Using the SAML-D dataset is a comprehensive and realistic solution for evaluation: its total number of transactions is 9,504,852 with 12 accurately selected features and 28 typologies: 11 normal and 17 suspicious. Of the transactions, only 0.1039% would be labeled as suspicious which makes it suitable for real-life AML cases thus guiding the development of improved models. The structure of the dataset is informed by review in the literature as well as consultation with AML specialists for higher relevance and utility. First, this dataset is rich in variety and more detailed than other normal datasets which improve the model's assessment and learning, Second, the proposed Federated Learning and CNN-GRU integration can find other simple but subtle money laundering pattern while at ensuring the privacy of every institution and also scalability.

4.2 Data Pre-processing

Normalization can work as mapping or scaling tool, that allows changing the range of values of a given feature. It is particularly beneficial as a preparatory step for prediction and forecasting models, where high variability is desirable, and data must operate within different but similar orders. Different methods of forecasting exist, and thus need proper normalization in order to improve the levels of precision and reliability in the forecasts. There are quite many traditional normalization methods that have been used most frequently which include Decimal Scaling, Z-Score, and Min-Max. However, there are new methods called the Integer Scaling technique to which these above methods can be replaced with. This new technique developed is based on the Advanced Min-Max Z-Score Decimal scale (AMZD) which is a new methodology for data normalization that differentiates it from others.

4.2.1 Min-Max Normalization

The Min-Max Normalization is an applied technique that maps all the data linearly to a fixed given range between a maximum and a minimum value. This also maintains relations contained within the initial datasets while at the same time normalizing the values so as to be within desired ranges. It is a simple, yet comprehensive solution to help standardize data to fit correctly with the macro or micro limits in a given project. The min max normalization approach is given in eqn. (1).

$$A' = \left(\frac{A - value\ of\ A}{value\ of\ A - value\ of\ A}\right) \times (D - C) + C \qquad (1)$$

Where, A' is the min max normalized data. C, D are the predefined boundary and A is the range of original data. unstructured data can be normalized using Z-score parameter gives in eqn. (2) and (3).

$$v_i' = \frac{v_i - E}{std(E)} \qquad (2)$$

Where, $v_i'$is value of the row E of i^{th} column.

$$std(E) = \sqrt{\left(\frac{1}{n-1}\sum_{i=1}^{n} \quad (v_i - E)^2\right)} \qquad (3)$$

Take for example five rows, i.e., X, Y, Z, U and V, and each represented by a variable or column designated by 'n'. The normalized values of each row are computed based on the Z-score approach. If a row has similar values, thereby making its standard deviation equal to zero, the values in that particular row are all set to zero. Similar to the Min-Max normalization approach, the Z-score also maps the values between the range 0 and 1.

4.2.2 Decimal Scaling

Decimal scaling is the process that creates a sequence between −1 and 1. Hence using the decimal scaling method, represented in eqn. (4).

$$v_j' = \frac{v_j}{10^j} \qquad (4)$$

Where, j is the smallest integer $max(|v|) < 1$.

4.2.3 Z-score Normalization

Through mean subtraction and standard deviation division, this process normalizes the data. It is now easier to compare data points with different scales because of this transformation, which ensures that the data has a mean of 0 and a variance of 1.

4.2.4 Decimal Scaling

This way the decimal point of the numbers is shifted to scale the data Depending on the measurement unit, numbers are scaled to build up ad hoc the needed measurement unit. The largest absolute value the number of decimal places which are changed corresponds, therefore as provided all values are within the normative scale of - 1 and 1. These techniques are employed so as to standardize data as follows: this confirms how different scales of data can be compared or processed together suing the same procedure. The document also suggests the new method called

Integer Scaling which is an extension of above all techniques. However, information is missing in the transcribed section especially in details.

4.3 Hybrid CNN-GRU for Anomaly Detection

4.3.1CNN-GRU

The CNN-GRU method suggested in the current paper integrates the functionalities of CNN and GRU to improve AML detection. CNN is used for the extraction of the spatial feature and pattern from the transaction data that is useful in detecting anomaly, which represents unlawful activities. At the same time, we use GRU, which is one of the Recurrent Neural Network (RNN), to identify temporal dependencies in the sequences and reversely examine the time-based subtlety of the fraudulent transaction sequences. This means that the proposed workflow also incorporates FL to the CNN-GRU model so that the model can be or trained by many financial institutions while preserving the privacy of the financial data. They can train the model locally on their own data compiled for internal use and only send the deltas to a central aggregator, hence protecting their precious financial data. It then forms these updates into a unified global AML system because the centralized model is effective. This architectural feature makes the design scalable, flexible and adheres to privacy requirements.

As a result, this work successfully implements the hybrid CNN-GRU model to attain higher efficiency and accuracy in identifying suspicious activities. As a result, it covers the spatial and temporal transaction pattern and would facilitate identification of intricate laundering activities. It is more efficient compared to the conventional methods of the AML and offers a solution to the globalization challenge in banking security fortification of financial systems.

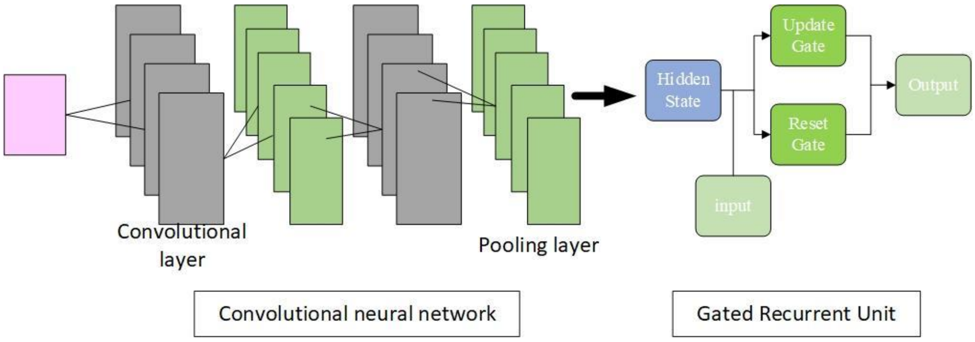

Fig.2 Architecture of proposed CNN-GRU Method

Fig.2 represents the CNN-GRU model intended for the multi-class classification that brought together CNNs and GRUs for use in intrusions detection. For spatial information extraction, there is a one-dimensional convolutional layer used for down-sampling; For sequence information processing component, this work employs a GRU network unit to process sequential data and avoid the problem of gradient explosion. The CNN-GRU architecture takes advantage of CNNs' power to identify small-scale relations and hierarchically arranged spatial structures, including transactional behavior, and the capacity of GRUs for capturing temporal relationships in chronological transaction series. Further sub layers, a roll-up layer, a dropout layer to encourages model's prevent overfitting, and an attention optimization layer enhance the classification outputs. Such a combination yields a stringent and optimized structure for the identification of outliers and potentially malicious activities to support more effective AML systems.

CNNs convolutional layer takes the input data and applies the learnable kernels to derive its features. Kernels are relatively small spatially, and they have to match in depth to the input (for example, 3x3x3 for 3-channel images). The convolution operation translates filters over the input and performs dot products to produce Activations Matrix of 2D, Stacked to form Output Volume. Individual neuron in the layer is connected to the small portion of input (receptive field) and the opinions of each neuron equal to size of the field. Other hyperparameters include filter size or depth, stride which determines how the filters slide across the input and zero-padding which controls the output dimensions. Eqn. (5) gives the spatial dimensions of the output volume.

$$output\ size = \frac{(V-R)+2Z}{S} + 1 \tag{5}$$

where V is the input volume size, R is the receptive field size, S is the stride and Z is the amount of zero padding.

It also discovered that the Gated Recurrent Unit (GRU), which is less complex compared to LSTM, yields positive results when working with different sequences such as, text, voice, and time series data. GRUs utilize three gates: there is update gate, reset gate, and current memory gate. The update gate regulates the passage of such knowledge to the future timeline and the reset gate decides the amount of information to forget. The current memory gate makes sure its input mean is zero, and minimizes the prior data effect. Compared with traditional RNNs, GRUs improve the vanishing-exploding gradient problem and apply to the tasks of natural language processing. Gate values are produced as a result of element-wise operation accompanied by sigmoid or tanh functions. GRU effectively solves the vanishing gradient problem and effectively learns the long-term dependency of a sequence in the data shown in eqn. (5), (6), (7), and (8).

$$z_t = \sigma(w^z x_t + V^z h_{t-1} + b^Z) \quad (5)$$

$$r_t = \sigma(w^r x_t + V^r h_{t-1} + b^r) \quad (6)$$

$$\underline{h}_t = tanh\big(w^c x_t + V^c(r_t . h_{t-1})\big) \quad (7)$$

$$h_t = (1 - z_t). h_{t-1} + z_t . \underline{h}_t \quad (8)$$

The update gate z_t produced when a sigmoid function is applied upon a dot product of initial input x_t and the future hidden state h_{t-1} controls the flow of data from the previous network to the subsequent network. The reset gate r_t is calculated in the same manner as the input gate, using sigmoid function and determines the amount of the previous state which is forgotten. In this equilibrium fashion, the gated mechanisms make GRUs enable to maintain and update important information throughout the long sequences.

4.3.2 Federated learning

“Federated Learning” (FL) is a learning technique in which several clients are used to train a model. Lecturer client developer Several clients exist consisting of sensors, mobile devices, and companies, for instance to develop a common global adequate model of social interaction without exchanging local data. Such clients perform local computations and offer only the model. updates (for instance gradients or weights of a model) to the server as opposed to reporting data back to a central server. As it is stated, by employing the numerous data that are scattered across clients this technique that also enhances data security and privacy aspects. Fig.3 represents the architecture diagram of federated learning.

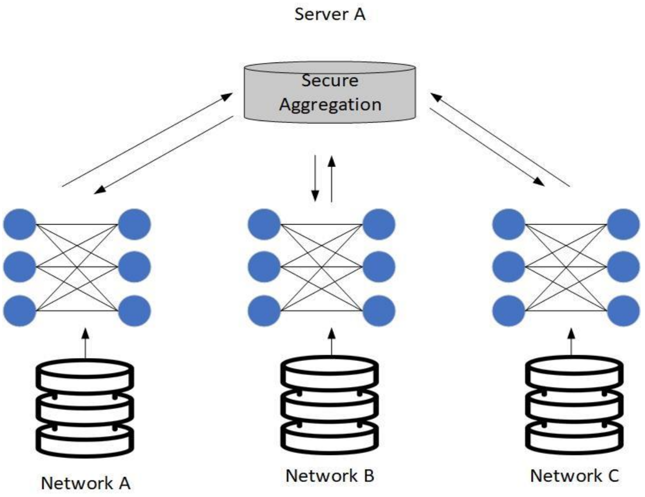

Fig. 3 Architecture of Federated Learning

In the process of federated learning, the shared or global model is updated more and more over time, accurate and robust. Each of the multiple clients of the software resides in different networks which are Network A, Network B and Network C, all clients have local data stored in their database. These clients update individual models while these computations are performed within the local area. Clients upload only model delta, i.e. a portion containing gradients or weights (parameters), to a central server, Server A. These updates are aggregated via secure techniques on Server A to form an enhanced global model. This cycle continues and at each iteration the updated global model is sent back to the clients for a further training process. This approach also maintains data confidentiality as original data is not sent to the cloud: only encrypted data in the format of coefficients.

RESULT

The proposed method suggests a new framework for “AML” that encourages the combined use of “FL”, “CNNs”, and “GRUs” in working to improve the security of global banking processes. Through Federated Learning, institutions can cooperatively train a machine learning model without sharing the data which is sensitive and violates the set regulation. Combining the two architectures, “CNN” and “GRU”, enhances the identification of the money laundering transactions by including efficiencies in both space and time. This work demonstrated that the proposed Federated “CNN-GRU” model provided faster and more accurate detection of anomalous activities compared to the traditional centralized system. This also enables future learning from other data sets than the current techniques used in money laundering. Based on the evidence, it would be rationale to point out that the examined model still has certain drawbacks, including temporal efficiency in terms of communication and processing loads. In the long run, this strategy enhances AML protocols that lead to creating more sound finances, and building trust.

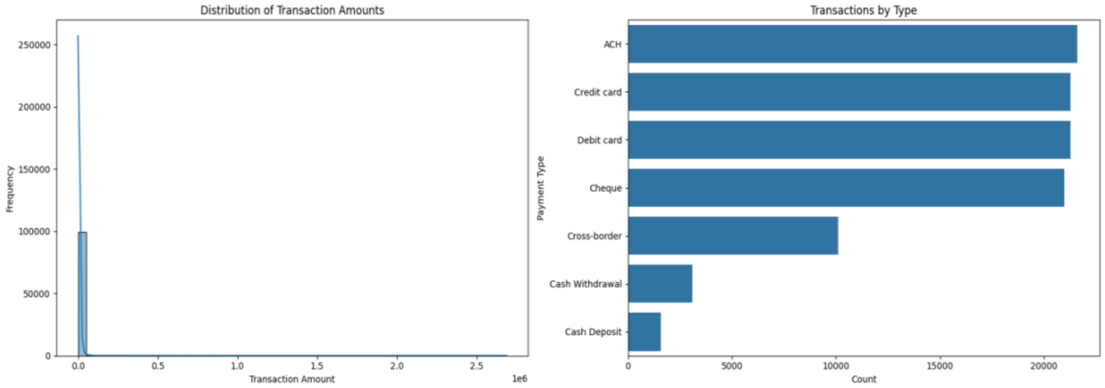

Fig. 4 Distribution of Transaction Amounts

Fig. 4 provide two visual representations of the transactions data. The first, histogram on the left, reveals the likelihood of the transaction amount. It shows a positively skewed one that means many more sales have been taking place at lesser price levels, as endorsed by the high frequency bar on the extreme left. A long tail is observable on the right and just goes up to 2.5 million; however, this shows that the number of transactions made at this level is much smaller than at other levels, which indicates that people prefer making high-valued transactions occasionally. The second graphic displays a horizontal bar chart on the right position and sorts the transactions by the payment type. This proves that ACH electronic transactions are most common followed by, credit/debit card transactions, cheque transactions. Other infrequent activities are Every time a transactor operates outside their home country or makes withdrawal or deposit. This chart also shows clearly that there are more electronic payment methods than the other forms of payment methods that are out there such as cheque and cash.

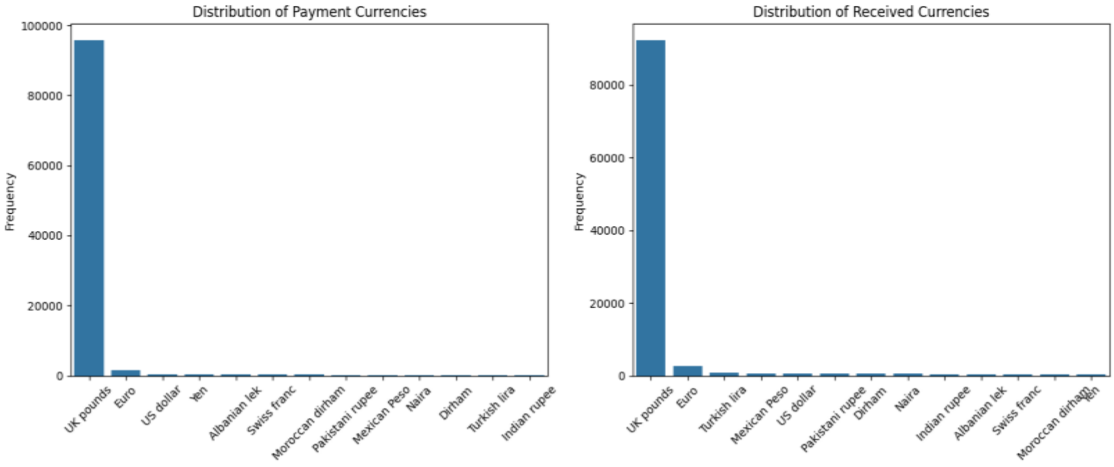

Fig.5 Distribution of Payment Currencies and Received Currencies

Fig. 5 synthesizes a bar chart of payments and receipts of transaction currencies. In both charts, the Pounds sterling is the most seen currency, generally representing 98 thousand of the overall transactions. Other currencies including Euro, US dollar, Yen as well as several others when compared to China have lower frequency indicating they are employed in small proportions when it comes to payment or receipts. It may be noted that UK pounds is same in both the charts because the financial transactions seem to be primarily regional, probably within UK and other currencies are not active in these types of transactions due to economic/operational reasons.

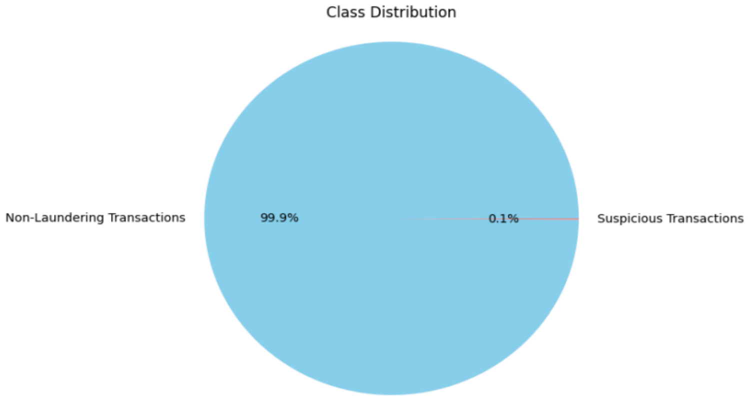

Fig.6 Class Distribution

Pie chart displayed in fig. 6 reveals the percentage of the different type of transactions in dataset. The world's largest slice, 99,9%, of transactions is neatly categorized under "Non-Laundering Transactions" effectively underlining the authenticity of most the transactions. However, a small portion with the title of Suspicious Transactions only constitutes 0.1%, which shows that such suspecting operations are very limited. This significant split underline the difficulty that financial institutions have in detecting money laundering, at the same time expressing the general sound and credible nature of the financial sector. At the same time, the chart proves that even if suspicious transactions are not numerous the monitoring has to be constant.

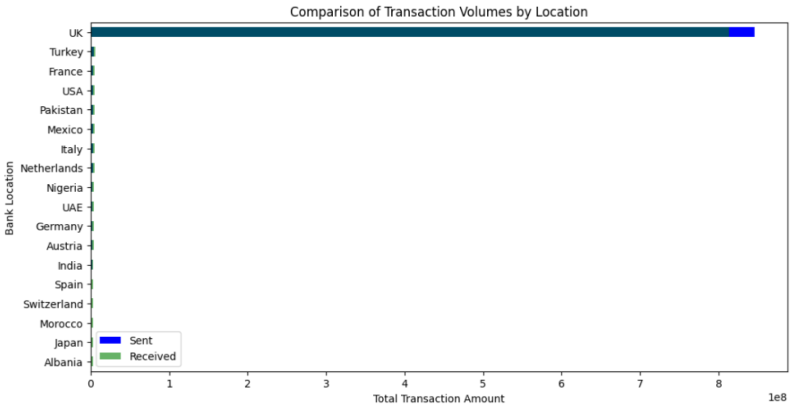

Fig.7 Comparison of Transaction Volumes by Location

The bar chart in fig. 7 compares the total amount of transaction volume for sending and receiving by country. On the x-axis, the transaction amount ranging between 0-800 million units are shown, and on the y-axis, it gives countries like UK, USA, France and Japan. Each country has two bars: One of the bars is a blue for the "Sent" transactions and the second bar is green for "Received" transactions. It is also clear when using the graph that one country is more of a sender or a receiver of a large number of transactions. It gives an understanding of the movements and directions of international financial activity.

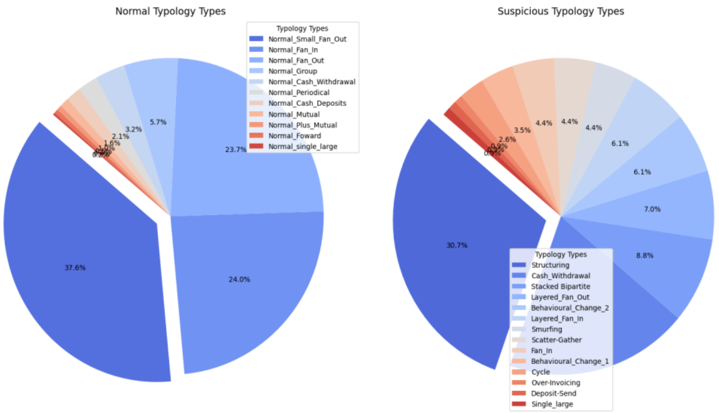

Fig.8 Normal and Suspicious Typology Types

Fig. 8 displays a side-by-side comparison of two pie charts: The first type is listed on the left as "Normal Typology Types" and the second type is on the right as "Suspicious Typology Types". The first bar chart represents one typology type as the largest blue section, meaning there is a recurring pattern in normal data other than anomalous cases. However, we can see the right chart with balanced categories illustrating the variety of suspicious activities observed. This contrast distinguishes between normal and suspicious cases regarding the distribution of typology; the former has dense areas, while the latter are good for fraud identification.

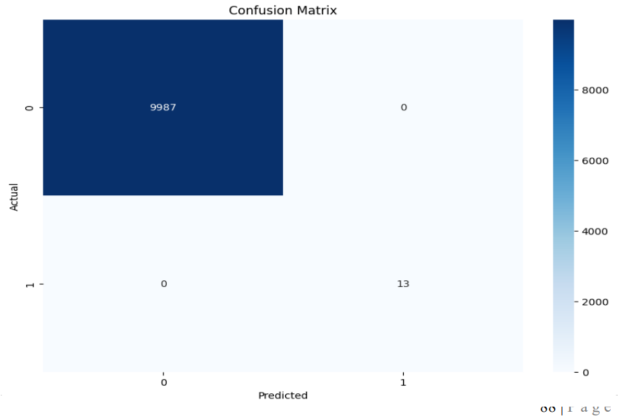

Fig.9 Confusion Matrix

Fig. 9 presents a confusion matrix, which is one of the main metrics for assessing the performance of classification models. It also categorizes a prediction against the actual class labels with rows being the true classes and columns as the predicted classes. A heatmap is used to represent the matrix which is prepared by using Python's matplotlib and seaborn libraries. By default, heatmap uses shades of colors for representation with number annotations added below to enhance its usability. Ways of labeling of the axes are appropriate ("Predicted" and "Actual") as well as the title of the graph chosen "Confusion Matrix". It also provides clear information about strengths within a model and how they relate to other features (diagonal features) as well as weaknesses in a model and how they relate to features (off-diagonal features) for model development.

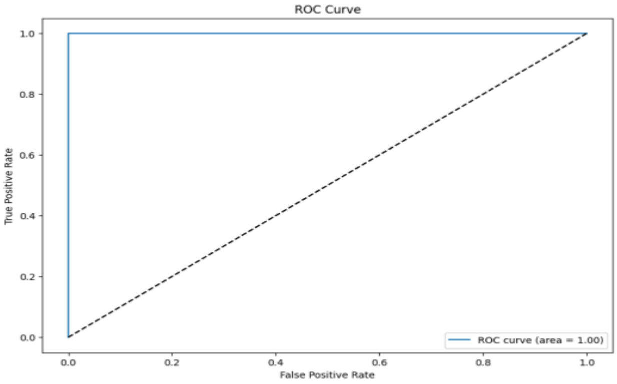

Fig. 10 ROC Curve

Fig. 10 illustrates an ROC curve as a way of analyzing the efficiency of a binary classifier at various decision rules. It charts the True Positive together with the False Positive, which gives information on how effective the model is at distinguishing between the positive and the negative classes. A classifier which has no over-testing error has an AUC of 1.00; in contrast a classifier with all the over-testing errors has an AUC of 0.5 as shown by the diagonal dashed line. ROC curves are very important not only in evaluating classifier's performance but especially for imbalanced datasets because a classifier with a higher AUC will have better discrimination between classes to help improve the model.

5.1 Performance Evaluation

Table I Comparison of Different Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
ANN	85.4	83.2	84.0	83.6
RNN	91.2	90.8	91.4	91.1
Gradient Boosting Regressor	91.6	89.5	90.2	89.8
KNN	87.3	85.0	86.1	85.5
PROPOSED CNN-GRU MODEL	98.7	97.5	98.2	97.8

Table 1 is a performance comparison of all the models employed for AML predictions using the proposed "CNN-GRU" model as the best model. According to the above listed models, moderate performance is realized by the "Artificial Neural Networks" (ANN), which is indicative of their capability of capturing intricate patterns from financial transactions. RNN has higher f accuracy and recall than Random Forest and Ada-Boost when employed in intruder detection, while Gradient Boosting Regressor has a higher f accuracy than other models. The last model is the "K-Nearest Neighbors" (KNN) model which is not good for scalability with higher dimensional data. The proposed "CNN-GRU" model outcompetes all the other approaches, where "CNN-GRU" model obtain an accuracy of 98.7%, precision of 97.5%, recall of 98.2% and F1-Score of 97.8%. This outstanding performance can be attributed for its advantage of combining "CNN's" function of spatial feature extraction with "GRU" that has a temporal dependency property. The findings confirm the reliability and flexibility of the developed "CNN-GRU" model in improving global banking security and recognizing various types of money laundering schemes.

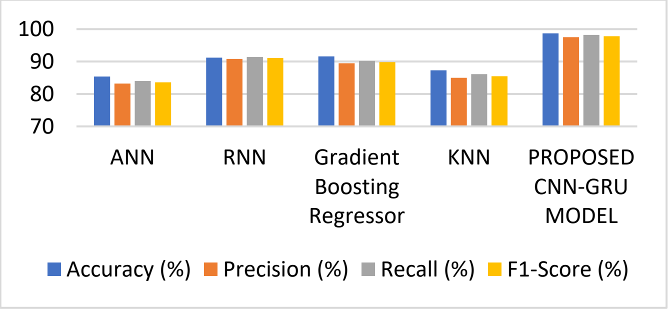

Fig.11 performance comparison of models

Fig.11 visually compares the performance of five models: ANN, RNN, GBR, KNN, and introduced CNN-GRU model. The length of each model is depicted by four bars in a row, each reflecting one of the measures to allow easy comparison. It can also be clearly observed from the chart that the proposed "CNN-GRU" model has higher accuracy than the other models. Nevertheless, according to the results obtained by the tested models, "KNN" demonstrates the lowest result. The compared models, RNN and Gradient Boosting Regressor, are located between the lower "KNN" and the higher "ANN" with slightly better performance of "ANN" than that of "KNN". The organization of this visualization successfully brings focus on the fact that the proposed "CNN-GRU" deliver better performance on the given task.

5.2 Discussion

The emergence and elevation of levels of money laundering remains a daunting task for the current global financial institutions and the regulatory authorities. Conventional methods of "AML" business controls are employed to either fail in its effort to detect suspected fraudulent transactions because they are time consuming, burdensome and may not be adequate at detecting new emerging money laundering techniques. The current techniques include rule-based systems and other conventional machine learning techniques like decision trees and support vector machines (SVM) that can hardly capture dynamic patterns or even temporal dependencies that exist in the sequence of financial transactions. However, even similar models entail the use of extensive labeled datasets which many times are hard to come by, especially in identifying very low frequency cases such as money laundering. As it has been demonstrated earlier, the proposed federated learning model combined with the hybrid "CNN" and "GRU" shows a much higher effectiveness compared to these basic approaches. The CNN component has a high efficiency in feature extraction, especially in analyzing the relationships between simple and compound characteristics of transaction data; the GRU model can effectively model time series data for detecting sequential money laundering activities. In addition, through federated learning, the model protects privacy and provides security since various institutions contribute to the model without transferring data information belonging to other organizations. This approach not only improves the model's scalability factor, but the issue of privacy is also well taken, which is an issue in the financial industry. The proposed hybrid model is found to be a more effective solution for identification of money laundering compared to the conventional machine learning and deep learning models. Indeed, it is superior to other models such as the decision tree and the SVM when it comes to working with large-scale and features many variables and being able to compare them based on periods of time. Thus, this work underlines the importance of further development of sophisticated, yet anonymized methods for AML detection, and the suggested "CNN-GRU" architecture is an important step toward achieving that objective.

CONCLUSION AND FUTURE WORK

The propriety of using Federated "CNN-GRU" models in AML systems means a revival approach to the improvement of the financial security. This method solves the most acute problems of confidentiality and privacy while working with delicate financial information in addition to enhancing the identification and combating of money laundering to a great extent. Given the fact that federated learning works independent of specific institutions, the process allows institutions cooperate with negligible data contamination or violation of existing regulation. CNNs as well as GRUs are regarded as highly efficient in extracting spatial as well as temporal features in the transactional data thus making it easy to detect incidences of fraudulent transactions. On the same note, the research also shows the feasibility of the model when adopted in diverse international banking situations. As such, the constant learning lays down a fordable and omnipotent approach against new and prevailing money laundering techniques, making the financial security future-proof. The challenges that require attention in the future are discussed below: The organization's communication efficiency and the overheads involved must be improved in the federated learning; hence, advanced method of compressing must be looked at, and the synchronizing protocols as well. Incorporating other types of financial data to the model, SNA & NLP, would add to the detection capabilities of the model. Also, assessing the approach's effectiveness using multi-jurisdictional and cross-country datasets will prove out its suitability. The features required for improving security will consist in stronger adaptations to differential privacy and federated averaging. In the long term, optimization of these technologies will address the dynamic needs of the global financial reforms.

REFERENCES

[1] D. P. Ramada, “Prevention of Money Laundering: Various Models, Problems and Challenges,” *Journal of Law and Legal Reform*, vol. 3, no. 1, pp. 67–84, 2022.

[2] D. P. Ramada, “Prevention of Money Laundering: Various Models, Problems and Challenges,” *Journal of Law and Legal Reform*, vol. 3, no. 1, pp. 67–84, 2022.

[3] T. Badics *et al.*, “Integral representation method based efficient rule optimizing framework for anti-money laundering,” *Journal of Money Laundering Control*, vol. 26, no. 2, pp. 290–308, 2023.

[4] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, “Fraud detection in banking data by machine learning techniques,” *IEEE Access*, vol. 11, pp. 3034–3043, 2022.

[5] F. Wan and P. Li, “A Novel Money Laundering Prediction Model Based on a Dynamic Graph Convolutional Neural Network and Long Short-Term Memory,” *Symmetry*, vol. 16, no. 3, p. 378, 2024.

[6] R. T. Potla, “Privacy-Preserving AI with Federated Learning: Revolutionizing Fraud Detection and Healthcare Diagnostics,” *Distributed Learning and Broad Applications in Scientific Research*, vol. 8, pp. 118–134, 2022.

[7] S. Kanamori *et al.*, “Privacy-preserving federated learning for detecting fraudulent financial transactions in japanese banks,” *Journal of Information Processing*, vol. 30, pp. 789–795, 2022.

[8] B. Guembe, A. Azeta, V. Osamor, and R. Ekpo, “A Federated Machine Learning Approaches For Anti-Money Laundering Detection,” *Available at SSRN 4669561*, 2023.

[9] A. A. Ahmed and O. Alabi, “Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review,” *IEEE Access*, 2024.

[10] Q. Yu, Z. Xu, and Z. Ke, “Deep Learning for Cross-Border Transaction Anomaly Detection in Anti-Money Laundering Systems,” *arXiv preprint arXiv:2412.07027*, 2024.

[11] S. Vasudeva Murthy, “Analysis on the significance and effectiveness of anti-money laundering policies and regulations of Financial Institutions (Investment Banks) in India,” PhD Thesis, Dublin, National College of Ireland, 2022.

[12] A. G. Kandachamy, “Overview of Anti-Money Laundering in the Banking Industry: An explanation of AML and the importance of it in the banking sector.,” *Management & Quality/Zarządzanie i Jakość*, vol. 5, no. 3, 2023.

[13] B. Sileshi, “Effectiveness of Anti-money Laundering Preventive Measures in Ethiopia: Case Study on Commercial Banks and Financial Intelligence Center.,” PhD Thesis, St. Mary’s University, 2022.

[14] A. Thommandru and B. Chakka, “Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks,” *Sustainable Futures*, vol. 5, p. 100107, 2023.

[15] H. Yi, “Anti-Money Laundering (AML) Information Technology Strategies in Cross-Border Payment Systems,” *Law and Economy*, vol. 3, no. 9, pp. 43–53, 2024.

[16] M. Liu, F. Kit Sam, J. Guan, and Y. Lau, “Implementing Anti-money-laundering Goals: New Technologies or Coordination between Related Agencies?,” *Journal of China Tourism Research*, vol. 18, no. 6, pp. 1284–1304, 2022.

[17] M. Issah, S. Antwi, S. K. Antwi, and P. Amarh, “Anti-money laundering regulations and banking sector stability in Africa,” *Cogent Economics & Finance*, vol. 10, no. 1, p. 2069207, 2022.

[18] H. Gandhi, K. Tandon, S. Gite, B. Pradhan, and A. Alamri, “Navigating the complexity of money laundering: anti–money laundering advancements with AI/ML insights,” *International Journal on Smart Sensing and Intelligent Systems*, no. 1, 2024.

[19] P. Gerbrands, B. Unger, M. Getzner, and J. Ferwerda, “The effect of anti-money laundering policies: an empirical network analysis,” *EPJ Data Science*, vol. 11, no. 1, p. 15, 2022.

[20] M. A. Zia, R. Z. Abbas, and N. Arshed, “Money laundering and terror financing: issues and challenges in Pakistan,” *Journal of Money Laundering Control*, vol. 25, no. 1, pp. 181–194, 2022.

[21] “Anti Money Laundering Transaction Data (SAML-D).” Accessed: Dec. 30, 2024. [Online]. Available: https://www.kaggle.com/datasets/berkanoztas/synthetic-transaction-monitoring-dataset-aml/data?utm_source=chatgpt.com