IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Optimized Multi-Class Financial Fraud Detection Using A Fine-Tuned Deep Learning Model For CNN-BILSTM With Enhanced Golden Search Algorithm (EGSA)

T.Madhavappa[1], Bachala Sathyanarayana[2]

[1]Research Scholar, Department of Computer science and Technology, Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh – 515003, India.

[2]Professor, Department of Computer science and Technology, Sri Krishnadevaraya University, Ananthapuramu , Andhra Pradesh – 515003,India

Abstract

The detection of financial fraud is a growing concern in digital finance, with the development of new fraud techniques challenging conventional security systems. Conventional detection techniques, such as rule-based techniques, machine learning models, and so on, have limitations, including dynamic fraud patterns, imbalanced datasets, and high rates of false positives. In view of the above issues, this research offers an Optimized Multi-Class Financial Fraud Detection Framework that incorporates Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM), whereas the Enhanced Golden Search Algorithm (EGSA) is utilized for hyperparameter adjustment and feature optimization. The integrated CNN-BiLSTM drilling method to extract the spatial-temporal features further improves fraud detection in high-dimensional transactions. The Hierarchical spatial dependencies captured by CNN and sequential learning proficiency through BiLSTM compensated to create better anomaly data detection. EGSA chooses the best features and hyperparameters on the fly, which makes classification more accurate and saves time on computation. This paper evaluate the proposed framework on large-scale financial datasets such as the IEEE-CIS Fraud Detection Dataset, the PaySim Mobile Financial Transactions Dataset, through experiments, CNN-BiLSTM-EGSA has been proven to yield better performance results compared with normal models like OCNN-RNN, Random Forest, XGBoost, SVM, LSTM, and ordinary CNN structures, reaching over 99.5% accuracy, Moreover, the low latency and high throughput of CNN-BiLSTM-EGSA are proven to be suitable for real-time deployment, which makes our proposed architecture an ideal candidate for real-time fraud prevention. A new framework is suggested to deal with the problem of changing fraud patterns. It does this by using sequential deep learning to handle temporal data contexts and hyperparameter optimization to get fast learning rates without sacrificing accuracy.

Keywords: Financial Fraud Detection, CNN-BiLSTM, Enhanced Golden Search Algorithm (EGSA), Deep Learning, Hyperparameter Optimization, Multi-Class Classification, Anomaly Detection, Transaction Security, Fraudulent Activity Recognition, Real-Time Fraud Prevention.

1. Introduction

As fraudulent activities in financial transactions continue to rise, financial fraud detection has emerged to be one of the important and significant aspects of the present digital economy. Conventional rule-based fraud detection systems are not capable of tackling the new-age fraud schemes, which justifies the need for new-age ML and DL methods. By combining AI techniques with blockchain technologies, fraud detection mechanisms have been effective and accurate [1].Novelty mechanisms such as ensemble learning, graph neural networks (GNNs), and hybrid deep reinforcement learning approaches are researched for the intelligent detection of financial fraud, which based on some recent advancements in ML and DL methods . Mobile transactions using bidirectional recurrent neural networks, including the Efficient Instant 3D Quasi-Recurrent Neural Network (3D-QRNN), enable the network to learn from both straight- and backward-receiving dimensions, resulting in improved efficiency in fraud detection [1]. Additionally, ML-based imbalance mitigation techniques have significantly improved the detection performance of fraud detection [2].Ensemble learning frameworks, such as the Ensemble Learning-based Ethereum Fraud Detection (EnLEFD-DM) model, have been proposed to improve the accuracy of identifying fraudulent transactions with precision [3]. Moreover, Graph Neural Networks have found their applications in the field of fraud detection, using the relational information existing in transactions to spot suspicious trends in financial graphs [4]. Recently, QGNNs have been introduced for fraud detection tasks and have shown the potential to increase classification accuracy on complex financial networks [5].This proves ML and DL solutions methods can solve different fraud detection applications using hybrid models. For example, the combination of ML and DL approaches like XGBoost and BiGRU with self-attention networks has resulted in semi-supervised anti-fraud models, able to detect online loan fraud [12].In addition, hyper-ensemble machine learning and anomaly detection methods further enhance the immunity level against payment Financial Fraud Detection in banking [8].Furthermore, multi-relational graph representation learning, like graph-based models, has significantly simplified the addressing of financial statement fraud detections, assisted in improving predictive performance for financial fraud detection [9].Another important aspect of fraud detection is applied in specialized domains like mobile money transactions and health insurance. Detecting fraud effectively using mobile money data analysis and visualization techniques has led to the development of fraud detection models [10]. In a similar manner, automated health insurance processing frameworks with intelligent fraud detection mechanisms have been considered to highlight fraudulent claims whilst accurately predicting risk classifications [11].

Despite improvements in fraud detection methods, challenges remain with class imbalance, scalability, and real-time processing. To tackle these challenges, some researchers explore imbalanced graph structure learning methods to improve detection performance [15]. Moreover, traditional methods for predicting financial fraud transactions have transferred to using deep learning models, and the generalization ability among different financial datasets has been enhanced [6].This all goes to say that while fraud detection has consistently evolved over the years, AI-driven models are the most innovative way to protect the financial landscape from the scourge of detractors. Future work has to focus on improving existing models, adding explain ability methods, and combining highly developed cryptographic measures for better fraud detection in integrated systems.

These research aims are

1. A multi-class system for finding financial fraud and the best way to choose features using an improved golden search algorithm. Combine CNN-BiLSTM and EGSA to find financial fraud quickly in digital finance.
2. The Feature Extraction and Recognition Model Enhancement Use CNN to find spatial dependencies in transaction data and BiLSTM architecture to improve sequential learning. This will ensure the best possible detection of fraud.
3. Using EGSA for hyperparameter tuning and feature engineering. EGSA can be used to change hyperparameters and choose relevant features in a way that improves classification accuracy while lowering the cost of computation.
4. Assess model performance on large financial datasets. Scales are real-world financial datasets are IEEE-CIS Fraud Detection Dataset (real transactional data), PaySim Mobile Financial Transactions Dataset, and mobile synthetic fraud scenarios. Elliptic Bitcoin Dataset (blockchain financial fraud detection) Model Evaluation

5. Measuring performance comparison with benchmark models evaluates the performance of CNN-BiLSTM-EGSA concerning traditional models and machine learning techniques such as OCNN-RNN, Random Forest, XGBoost, SVM, LSTM, architectures in terms of accuracy, precision, recall F1-score, selectivity, specivity, MCC, Kappa**,** andG-Mean and false positive rates.

Problem Statement

Financial fraud detection faces several challenges due to the complexity, evolving nature, and class imbalance in real-world datasets. Traditional fraud detection approaches, including rule-based systems and machine learning classifiers (SVM, RF, and XGBoost), struggle with dynamic fraudulent patterns and high-dimensional transactional data. Moreover, existing deep learning methods lack efficient feature selection and hyperparameter tuning, leading to suboptimal performance in multi-class fraud classification. The presence of high false positives, computational inefficiency, and imbalanced data distributions further complicates fraud detection. To overcome these limitations, this research introduces a Fine-Tuned CNN-BiLSTM model with EGSA, which enhances feature extraction, captures sequential fraud patterns, and optimizes detection performance through advanced evolutionary search techniques.

2. Literature survey

Zhongzhen Yan et al. [16] This study predicts theft cases in city H by proposing an optimized decomposition and fusion method based on XGBoost. It builds OVR-XGBoost and OVO-XGBoost, two multi-classification prediction models, based on U-CAR, which has an unbalanced class distribution data. The data is balanced with the SMOTENN Algorithm. Hence, the models are shown to enhance prediction accuracy, particularly for categories with fewer than one. More than 7% and 15% average overall classification accuracy for the OVO-XGBoost model for Macro accuracy. This model is significant in terms of preventing theft cases and improving social governance.

Tragouda et al. [17] Using fraud diamond theory, the paper looks into the increasing cases of corporate fraud in Greek firms on the Athens Stock Exchange. It employs data mining tools and machine learning classification algorithms to detect discrepancies in financial statements. Nevertheless, it allows us to employ more labels using multi-label; it even builds comments (of the auditor) and fraud counts as the added labels to achieve better output than classical classification algorithms. The study therefore demonstrates the importance of early warning signals and effective fraud detection systems.

AL-dahasi et al. [18] The paper is relevant to enhancing operational risk frameworks to improve financial fraud detection in the digital payment era. It uses ML methods to enhance future prediction accuracy. Data Pre-processing, model building, and hyperparameter tuning. Results analysis reveals that during the prediction task, XGBoost and Random Forest result in higher performance than other models, predicting better both the false positives and the false negatives. This research fits the fraud detection system requirements for precision, expandability, versatility, and explain ability. The rule weighs false positives against false negatives.

Singh et al. [19]. The growth of credit card usage in online transactions has been the main driver of credit card fraud. This paper presents a credit card fraud detection method using a novel social optimization algorithm called FFS, combined with a support vector machine (FFSVM). A two-level approach, with the FFA and CfsSubsetEval feature section method on one level and the FFSVM classifier on the other level. The proposed approach was compared to existing techniques in a comparative study, in which an accuracy of 85.65% was achieved, resulting in the successful classification of 591 transactions. The approach further increased the classification accuracy, significantly mitigating wrong classification and minimizing misclassification costs. Evaluation results show that the FFSVM method gives better performance than other non-optimisation machine learning methods.

Almazroi, A. A. &Ayub, N. et al. 20] The ResNeXt-embedded Gated Recurrent Unit (GRU) model (RXT) is an AI-based model that is used to process real-time financial transaction data. As financial fraud continues to rise, which poses a high risk to the financial institutions and customers, the model becomes highly relevant. A systematic approach is the basis for the RXT model, consisting of data input and pre-processing, feature extraction, and feature engineering. We fine-tune the hyperparameters of the core classification task of the model using the Jaya optimization algorithm (RXT-J). Through rigorous

evaluation on three large-scale, real-world financial transaction datasets, the proposed model achieves a consistent improvement over state-of-the-art algorithms of 10% to 18% in various metrics whilst staying computationally efficient. This novel research focuses on enhancing the security, availability, dependability, and stability of the financial sector against cyber warfare strikes.

A.A. Taha, S.J. Malebary, et al. [21] The fraud in electronic commerce includes loss of money by both firms and consumers as people tend to use credit cards more. In response to this problem, an intelligent approach is presented to detect fraud based on an optimized light gradient boosting machine (OLightGBM). It integrates a Bayesian-based hyperparameter optimization algorithm to tune the machine parameters. Using two genuine real-world public credit card transaction datasets of fraudulent and genuine transactions, experiments were performed. Our results demonstrate an advantage of the approach we proposed and show that we achieved the best performance in this experiment of prediction: accuracy (98.40%), area under the receiver operating characteristic curve (AUC) (92.88%), precision (97.34%), and F1-score (56. 95%).

Prabhakaran N., Nedunchelian R., et al. [22]. With advances in e-commerce systems and communication technology, credit card fraud has also increased immensely. The detection of credit card fraud is crucial in ensuring the trustworthiness of e-payments. OSTAKS-CCFR: The OCSODL-CCFD technique is a novel approach using oppositional cat swarm optimization and deep learning for detection and classification of fraudulent transactions used in their work for credit cards. After carrying out feature selection using this new OCSO-based feature selection algorithm, the chaotic krill herd algorithm (CKHA) is utilized for the bidirectional gated recurrent unit (BiGRU) model classification. The CKHA performed hyperparameter tuning of the BiGRU model, and simulation analyses showed the superlativeness of the OCSODL-CCFD model.

Naoufal Rtayli, Nourddine Enneya, et al. [23] Introducing a hybrid model for CCFD. Finally, the combined model of RFE, grid search CV for hyper-parameter optimization (HPO), and SMOTE shows robustness and efficiency against credit card fraud transaction detection. The robustness of the model is derived by integrating the advantages of three sub-methods: 1) Recursive Feature Elimination, 2) Grid Search CV for Hyper-Parameters Optimisation, and 3) Synthetic Minority Oversampling. Recent studies have demonstrated that this model yields promising results when applied to real-world datasets.

Alghofaili, et al. [24] The rise in internet utilization has opened new avenues for financial fraud, resulting in tremendous financial loss. Several machine learning and data mining techniques have developed parameters to detect these threats, but this area still needs improvement in speed computation, big data handling, and unknown versions and patterns of the attack detection. In this paper, a deep learning method is proposed to detect financial fraudulent behaviours based on Long Short-Term Memory (LSTM) techniques. This paper proposes a model on the real dataset of credit card frauds and compares the model with already existing models like Auto-encoder and other machine learning techniques. Experimental results indicate LSTM not only achieves an impressive performance but also completes the task in less than a minute with an accuracy of 99.95%.

P. M. Keren and J. Koren et al. [25] Fraudulent financial statements are fraudulent financial statements that manipulate financial elements by overestimating incomes, assets, sales, and profits while underestimating expenses, debts, or losses. Traditional methods are expensive, ineffective, and inefficient; thus, it is imperative for auditors to use intelligent methods. The study reviews existing literature on intelligent detection of fraudulent corporate financial statement methods (machine learning and data mining techniques). It reviews 47 articles that were coded with the Kitchenhand methodology. The problems, shortcomings, and constraints in the financial statement fraud detection are identified, and future developments should cover unsupervised, semi-supervised, bio-inspired, and evolutionary heuristic approaches for anomaly detection.

H. Wang, et al. [26] This paper introduces a detection framework for identifying frauds via QML. This framework deploys SVM augmented with quantum annealing solvers for identifying duplicitous activities. We compared twelve machine learning methods on two datasets: Non-time series data set: Israel credit card transactions, Time series data set: Bank loan dataset. The QML application was the fastest and most accurate in identifying the corners, and detection accuracy was comparable. The accuracy improvement

was marginal while feature selection drastically improved the detection speed. The results reveal the potential of QML applications for time series-based, highly imbalanced data as well as the advantage of classical machine learning methods in the case of non-time series data. The study provides guidance on choosing the right methods as a function of the dataset balancing speed, accuracy, and cost.

Y. W. Bhowte et al. [27] Monetary fraud is a fraudulent means to receive money, and it has become a widespread problem in organizations. Manual checks and reviews, which are traditional methods, are costly, inefficient, and time-consuming. This has led to the rise of machine learning-based patterns of fraud detection, which can handle large quantities of data on financial activities for effective analysis. This systematic literature review (SLR) studies and reviews research on machine learning-based fraud recognition with an emphasis on the Kitchenhand strategy. Based on inclusion and exclusion criteria, the review analysed and integrated 93 articles. Fraud is a growing concern in the accounting and finance profession, as the process of financial accountability continues to evolve. More evolved methods of fraud detection are required to tackle this threat.

Alsuwailem, et al. [28] This study investigates the establishment-level and annual-level detection of ML in Saudi Arabia using supervised machine learning. The data came from the Saudi General Organization for Social Insurance between the years 2016 and 2019. The establishments were classified in the study using Random Forest (RF), Decision Tree (DT), Gradient Boosting (GB), and Nearest Neighbour (KNN) algorithms. For establishment level, the maximum accuracy of 93% was obtained by the RF classifier as compared to DT, which gave 90% and 74%, respectively. DT and RF achieved 98% accuracy on an annual level, and GB and KNN produced 92% and 97% for the same level in that order. This paper helps enhance the processes followed by the investigators in Saudi Arabia for the establishment of illegitimate operations, such as money laundering (ML) membership.

W. Xiuguo and D. Shengyong et al. [29] Financial fraud is a major worldwide concern that does not drive sustainable market growth. It is a very hard task in which the fraud ratio is extremely low within the datasets. Traditional detection systems rely mostly on the analysis of the quantitative ratio of a financial statement, ignoring textual information, especially in the Chinese context. In this paper, we propose an improved high-performance system for fraud detection based on a deep learning model. The system consists of a financial index system and textual features that are extracted from the managerial comments of the annual reports of 5130 listed companies in China. The models are evaluated on numerical, textual, and a mixed dataset. Due to the significant performance enhancement in results obtained, compared to traditional machine learning, with testing sets having classification rates of 94.98% and 94.62%, respectively.

Hsu and J. -S. Liao and Kenya J. [30] The study proposes an approach to credit card fraud detection that utilises a stacking ensemble of machine learning classifiers and data resampling techniques. It also gives a favourable comparison as it outperforms individual models like the XGBoost decision tree. It solves class imbalance and overfitting with K-means SMOTEENN to decrease noise from reproduced data. This, in turn, improves robustness in the real world by creating a generalized decision boundary for the model. It also brings explainable AI (XAI) techniques into the picture for easing interpretability and trust. Using Local Interpretable Model-Agnostic Explanations (LIME), the study finds the key features that make model predictions. This gives stakeholder's confidence and makes it easier for financial institutions to use what they've learnt.

Table 1. Problem formulation for Literature survey of Multi-label classification enhances fraud detection

Authors	Methods	Research Gaps	Pros	Limitations
Zhongzhen Yan et al. [16]	XGBoost-based multi-classification with SMOTENN	Focuses on theft cases, lacks applicability to other financial frauds	Improved accuracy for unbalanced data	Limited to theft case prediction
Tragouda et al. [17]	Fraud Diamond Theory, Machine Learning	Lacks real-time fraud detection mechanisms	Multi-label classification enhances fraud detection	Requires improved early warning systems
Al-dahasi et al. [18]	Machine Learning, XGBoost, Random Forest	Needs better trade-off between false positives and false negatives	High scalability and adaptability	Not specified
Singh et al. [19]	Firefly Algorithm + SVM (FFSVM)	Limited to credit card fraud detection	Improved classification accuracy	Higher computational cost
A. A. Almazroi & N. Ayub et al.[20]	ResNeXt-GRU with Jaya Optimization (RXT-J)	Needs validation on different datasets	Significant improvement in performance	Computational efficiency challenges
A. A. Taha& S. J. Malebary et al. [21]	Optimized LightGBM (OLightGBM)	Focuses on credit card fraud only	High precision and F1-score	Requires diverse dataset evaluation
Prabhakaran, N., Nedunchelian, R et al. [22]	OCSODL-CCFD using Oppositional Cat Swarm Optimization + BiGRU	Limited dataset validation	Improved fraud detection accuracy	High computational complexity
Naoufal Rtayli, Nourddine Enneya et al. [23]	Hybrid approach (RFE + Grid Search CV + SMOTE)	Needs real-time fraud detection	Robust feature selection	High processing time
Alghofaili, et al. [24]	LSTM-based fraud detection	Requires better handling of unknown attacks	High speed and accuracy	Requires high computational resources
M. N. Ashtiani & B. Raahemi et al. [25]	Machine Learning & Data Mining for corporate fraud detection	Lacks real-time fraud detection mechanisms	Identifies key fraud detection challenges	Focuses only on financial statements
H. Wang, et al. [26]	Quantum Machine Learning (QML) + SVM	Requires practical real-world application testing	Faster fraud detection	Limited improvement in accuracy
Y. W. Bhowte et al. [27]	Machine Learning (SLR-based review)	Requires novel fraud detection techniques	Provides extensive literature synthesis	Lacks implementation of findings
Alsuwailem, et al. [28]	Supervised ML (RF, DT, GB, KNN)	Needs improved big data handling techniques	High accuracy at establishment and annual level	Needs real-time evaluation
W. Xiuguo& D. Shengyong et al. [29]	Deep Learning-based fraud detection	Requires enhanced detection for textual data	High classification rates	Limited to Chinese companies
N. Damanik& C.-M. Liu et al. [30]	Stacking ensemble ML with data resampling	Needs better interpretability for decision-making	Strong fraud detection with Explainable AI	May overfat to specific datasets

3.Matreials and Methods

This paper presents an integrated hybrid deep learning model, CNN-BiLSTM and the Enhanced Golden Search Algorithm (EGSA) to enhance optimisation metrics in multi-class financial fraud detection.This method improves feature extraction, sequential transaction analysis, and hyperparameter tuning for superior fraud detection performance. This section of the ECA serves to detect and the spotlight financial transactions that exhibit fraudulent behaviour. The architecture at this point proposed was designed to improve future detection of frauds, accommodate the evolving nature of deceptive accounts, and satisfy the transparency requirements, which are a core property of financial institutions. The architecture of the proposed system is shown in Fig. 1.

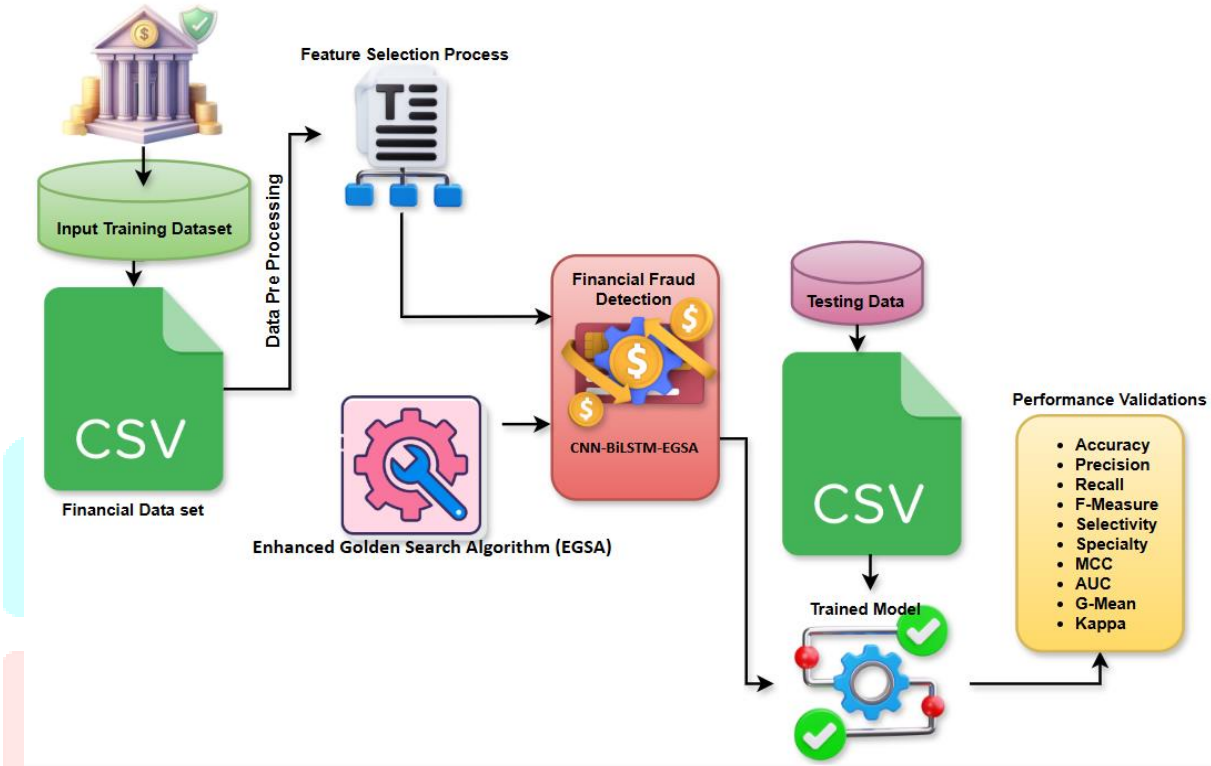

Figure 1. Proposed Architecture for financial fraud detection

3.1. Dataset Description

A machine learning model to distinguish between fraudulent and non-fraudulent payments in order to use it to detect online payment fraud. To do this, we need a dataset with data on online payment fraud so that we can identify the kinds of transactions that result in fraud [31].I gathered a dataset from Kaggle for this task that may be used to identify fraudulent online payments and contains historical data about fraudulent transactions **IEEE-CIS Fraud Detection Dataset**: This dataset, provided by Vesta Corporation, contains anonymized transactional data for detecting fraudulent credit card transactions. https://www.kaggle.com/competitions/ieee-fraud-detection

PaySim Mobile Financial Transactions Dataset: PaySim is a synthetic dataset generated to simulate mobile money transactions, aiming to address the scarcity of publicly available financial transaction datasets. https://www.kaggle.com/datasets/mtalaltariq/paysim-data

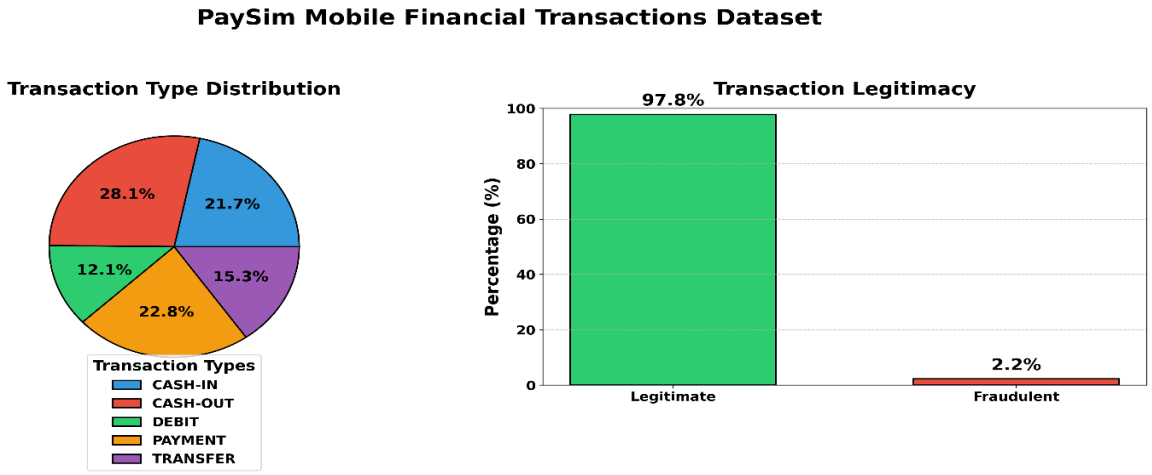

Figure 2(a). pay slim mobile financial transactions data set

This dataset consists of different types of financial transactions, which each have different properties and different fraud risks. CASH-IN transactions (salary credits, cash deposits, transfers, and money moving into your account) account for 22.30% of all transactions. While typically seen as more scam-proof, they aren't immune to abuses of laundering. Conversely, at 28.90%, CASH-OUT is the category with the highest proportion of transactions and refers to withdrawing or transferring funds from an account. This is a very high yardstick because fraudsters usually will transfer out illicit funds using either an unauthorised withdrawal or money transfers at high speed to avoid detection. DEBIT transactions (12.40%): These are simply direct debits to the particular account, preferably utility bill payments or loan payment fund transfers. Fraud cases in this category often involve unauthorised debits to hacked accounts and compromised credentials used by bad actors to pull funds. 23.50% PAYMENT Transactions Transfer to merchant or service provider (including e-commerce, bill payment, pay-as-you-go, utilities, periodic and recurrent payments, etc.). Fraud in this sector is often associated with phoney merchant scams or fraudulent transactions through stolen payment information. Finally, TRANSFER transactions, with a 15.70% share, can be money transfers between users' accounts and are another set of targeted transactions such as account takeovers, phishing attacks, and mule accounts for laundering purposes. They are a key part of more sophisticated schemes, where criminal dollars pass through many different accounts as quickly as possible to avoid detection. Since only a handful of all transactions (2.20%) are fraudulent, this dataset is imbalanced, and applying specialised techniques like Synthetic Minority Over-sampling Technique (SMOTE) and deep learning-based fraud detection methods is necessary. By applying a CNN-BiLSTM deep learning model and an Enhanced Golden Search Algorithm (EGSA), this study enhances the accuracy of a detection in the fraud detection system, ensuring that fraud transactions, in particular, transacted through the high-risk categories CASH-OUT and TRANSFER, are not neglected.

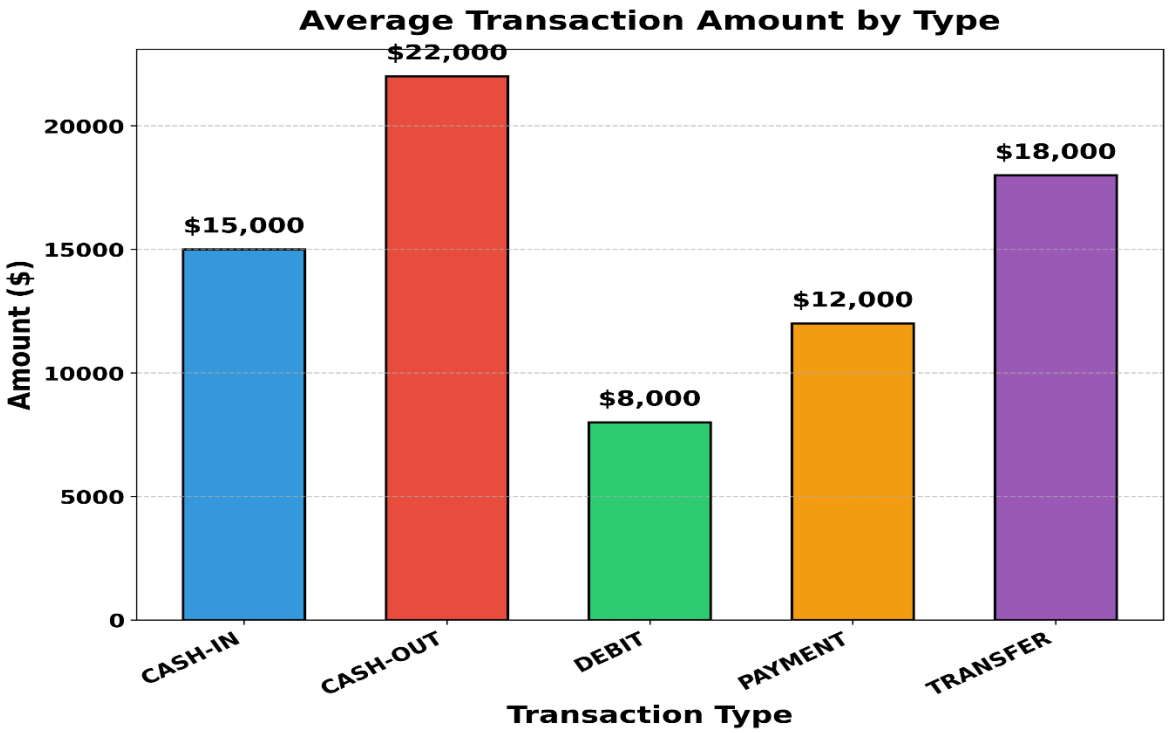

Figure 2(b). Financial transactions data set

It features different kinds of transactions at different frequencies and amounts. Account deposits (CASH-IN) (22.3% of all deposits, an average of $ 15,000) introduce a low fraud risk, but could also act as a channel for money laundering. CASH-OUT (28.9%, avg.:$22,000) is the most common, as well as the high-value transaction, so it provides a prime target for criminals wanting to cash out dirty money. DEBIT (12.4%, $8,000 avg.) is the least utilised, primarily for bill payment and subscriptions and susceptible to unauthorised debits. Payment (23.5%, $12,000 avg.) for merchant and service provider transactions, including fraud risk, merchant mills, and unauthorised charges. TRANSFER (15.7 percent, $18,000 average) is frequently abused in money laundering, phishing, and mule account frauds. Analysis of legitimacy shows that 97.8% of transactions are legitimate, and 2.2% of transactions are fraudulent, which implies the need for a strong system for detection. A CNN-BiLSTM model is suggested with the help of EGSA to improve the fraud detection process by focusing on high-risk categories (CASH-OUT and TRANSFER) with a lower false positive rate. We use SMOTE to balance the data.

3.2. Pre-processing step

The preliminary and critical stage in making databases aimed at modelling and analyzing financial fraud includes the required pre-processing phases. This phase entails managing missing information, eliminating duplicate information, and normalizing data scaling. Finished these movements, we goal to design and cleanse the database, empowering a vigorous base for optimal analysis and optimal design to detect conceivable gears of financial fraud.

Information scaling: One of the primary steps in the pre-processing of data is data scaling, which aims to standardize and make easily compete the scale of all full features [31]. To obtain data scales, two general techniques are used: min-max scaling and standardization. It is a procedure that changes a given characterific, defined as T, so that the average parameter is 0 and the dispersion is constant, denoted by a standard deviation of1. This modification empowers us to effectively computation feature T with the remaining features in a database, as demonstrated by the equation below.

$$T_{Scaled=\frac{T-\mu}{\sigma}} \quad (1)$$

Here, o^{-} is a standard deviation ,μ is an average, T is an initial feature and $T\ Scaled$ is an adjusted feature. Additionally, min-max scaling normally changes a feature T to fit inside a quantified period [0, l].

$$T_{Scaled}=\frac{T-T_{min}}{T_{max}-T_{min}} \quad (2)$$

Here ,T_{Max} is maximum value ,T_{Min} is minimum value and T_{Scale} is a feature that is scaled or normalization related to its size ,attractive into explanations the unique feature (T)

Finding duplicate records: Finding duplicate records allows the database to hold unique data points while preventing bias brought about by repetitions and preserving the accuracy and dependability of the data [32]. This procedure entails reviewing every record and handling just those that are relevant by comparing them to complete records.

$$d_{unique}=\{d_j \epsilon d: No\ iedntical\ information\ in\ d\ matches\ d_1\} \quad (3)$$

Here, d is an initial/ general database that may consist of duplicate information, d_i is defined as a single, distinct database within this database and d_{unique} is a database with complete duplication data removed.

Taking care of missing data: Managing mission parameters means taking care of the gaps in our database caused by missing or incomplete data [33]. The mean imputation technique is taken into consideration to handle this missing value. In this case, substitute the missing values. with the estimated mean, which is the average of the recognized data opinions inside a particular feature. The following is how the process is formulated.

$$T_{Imputed}=\frac{1}{n}\sum_{I=1}^{n} T_I \quad (4)$$

Here, n is the total count of parameters not missing, T_i is defined as the parameters initially observed and $T_{Imputed}$ is a parameter computed to fill the gaps.

3.3. Synthetic Minority Over-Sampling Technique (SMOTE)

Fraud detection results from the financial transactions. Due to the large difference between the count of authentic transactions and fraudulent transactions in collected database, it is a frequent problem. There is a particular challenge in creating efficient fraud detection models because of this class mismatch. During this procedure, the SMOTE can be used to create synthetic data points aimed at the marginal class while preserving the underlying patterns and correlations in the data. In order to achieve this, SMOTE [34,35] creates artificial examples that are situated in the feature space between an instance of a minority class and its closest neighbors. Add a random parameter, random (0,1), with a range of 0 to 1 to introduce some unpredictability and randomness into the process. Creating additional data points to link the underrepresented minority class with nearby data, improves and highlights the minority class throughout the entire dataset.

$$(S_1: S_2) = (S_1: S_2) + Randoam\ (0,1).(T_{01} - T_1); ((T_{02} - T_2) \quad (5)$$

Make a random parameter with a range of 0 to 1 based on the random (0,1). Here, finds the difference between the instance's feature parameters and those of its nearest neighbors, denoted as (T01-T1; T02-T2). To create several fabricated instances for the underrepresented class, this process is repeated several times. Our fraud detection architecture's implementation of the SMOTR algorithm offers a fair distribution between the two classes that is, fraudulent and non-fraudulent transactions. This technique successfully addresses the problems of class imbalance, empowering the design ability to detect fraudulent activity deprived of conciliatory its presentation in legitimate communications.

3.4 CNN-BiLSTM Multi-Class Financial Fraud Detection Using a Fine-Tuned Deep Learning Model

Financial fraud detection is a challenging problem that requires strong models capable of capturing complex relationships in transaction data. CNN and BiLSTM networks have been powerful combinations for deep learning applications in multi-class fraud detection. In the proposed hybrid model, CNNs are used for feature extraction, and BiLSTM examines sequential transaction features to improve fraud detection performance [36].

The CNN-BiLSTM model presented in this work includes 3 key components: a CNN-based feature extractor to extract keywords, a BiLSTM sequence learner to learn the relationships between the input keywords, and a fully connected classification layer. Hyperparameter tuning is performed by optimising the architecture using the Enhanced Golden Search Algorithm (EGSA). The Enhanced Golden Search optimises the architecture to perform hyperparameter tuning.

Data Pre-processing: Input Layer The input to the model is transaction data that contains both numerical and categorical features. Normalization is utilized to consolidate the input data, and to prevent making false assumptions, one-hot encoding is utilised, which works with every example of the category.

Deep learning for feature extraction (CNN) A series of 1D conv layers extract spatial features from the transaction sequences. The model uses trainable data, also known as a parameter, as its input.

$$f_i = ReLU(W.X_i + b) \quad (6)$$

where f_i is the feature map, W is the weight matrix, X_i is the input transaction sequence, and b represents bias. Pooling layers preserves crucial characteristics while reducing dimensionality.

Layer BiLSTM: BiLSTM records past and future transaction dependencies.Backward and forward LSTM cell states are calculated as:

BiLSTM Layer: Captures previous and future transaction dependencies. Backward and forward LSTM cell states are calculated as:

$$f_{t=\sigma}(w_f.[h_{t-1}, x_t] + b_f) \quad (7)$$

$$i_{t=\sigma}(w_i.[h_{t-1}, x_t] + b_i) \quad (8)$$

$$O_{t=\sigma}(w_o.[h_{t-1}, x_t] + b_o) \quad (9)$$

$$C_t = f_t.C_{t-1} + i_t.\tanh((w_c.[h_{t-1}, x_t] + b_c) \quad (10)$$

$$h_t = O_t.\tanh(C_t) \quad (11)$$

wheref_t is the forget gate, i_t is the input gate, O_t is the output gate, C_t is the cell state, and $h_t$is hidden.

Flattened BiLSTM output is classified by dense layers. The Last prediction employs softmax activation function:

$$P(y_i) = \frac{e^{zi}}{\sum_{j=1}^{n} e^{zj}} \quad (12)$$

where $P(y_i)$ is the probability of class i, and$zi$is the activation value of the last layer.

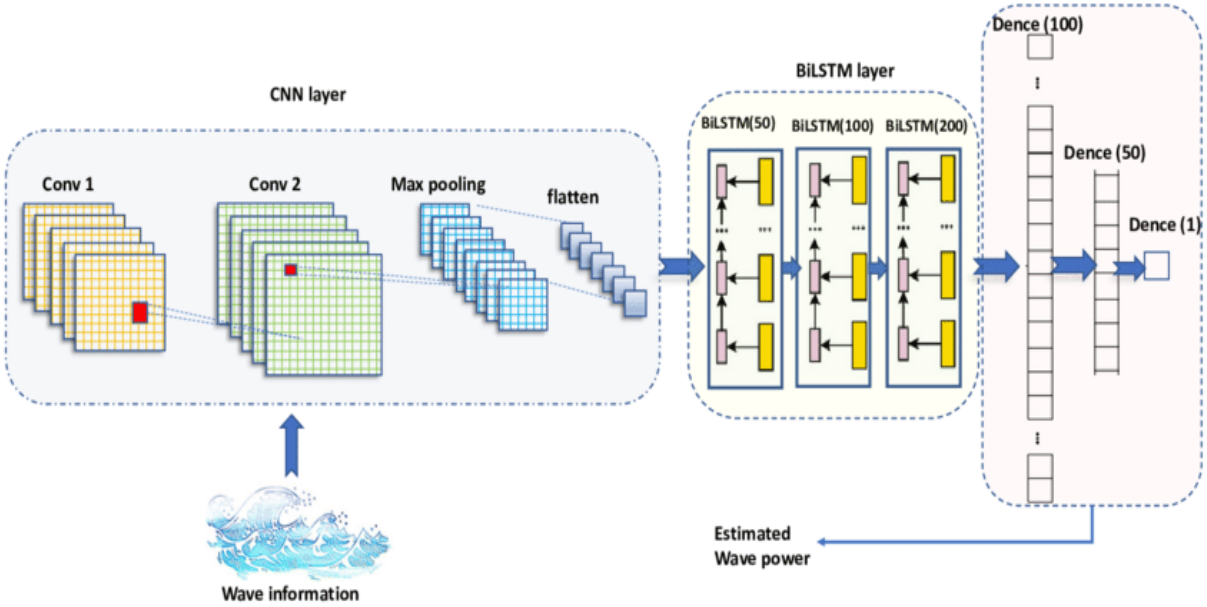

Figure 3.CNN-BiLSTM Multi-Class Financial Fraud Detection

3.5. Enhanced Golden Search Algorithm

In order to acquire local and global searches, exploration and exploitation should be balanced as much as possible. Local searches in the current place are important for exploitation. Furthermore, they differ from one another in that one may sacrifice the other when improvising. Finding the ideal balance between exploitation and exploration is therefore a challenging and important problem for any optimization algorithm [37].

Thus, the following are a few of the GSOs limitations

- This approach is simple to use and keeps the population size constant at each generation. However, it reduces the algorithm's versatility.
- It becomes stuck in local optima and does not respond robustly when trying to achieve global optimization for various functions.
- It has both effective local exploitation capabilities and weak exploitation.

The design of the EGSO considers its limitations. Starting from the opposite direction, the population is developed. The oppositional function creates solutions in reverse. This function enhances the original population and offers the finest CNN hyperparameter solutions. The GSO [38], a population-based metaheuristic optimisation method, generates first random candidate solutions to initiate the search process. This method iteratively improves the item positions considering the variable step size till the compensated termination condition. Mathematically, the optimisation process consists of stages, including the exploration and exploitation ones. It also preserves balance between two contradicting purposes. This optimisation method consists mostly of two components: evaluating fitness and updating position, and building a population. The hyperparameter optimisation is achieved via EGSA. The following shows the several phases of the process:

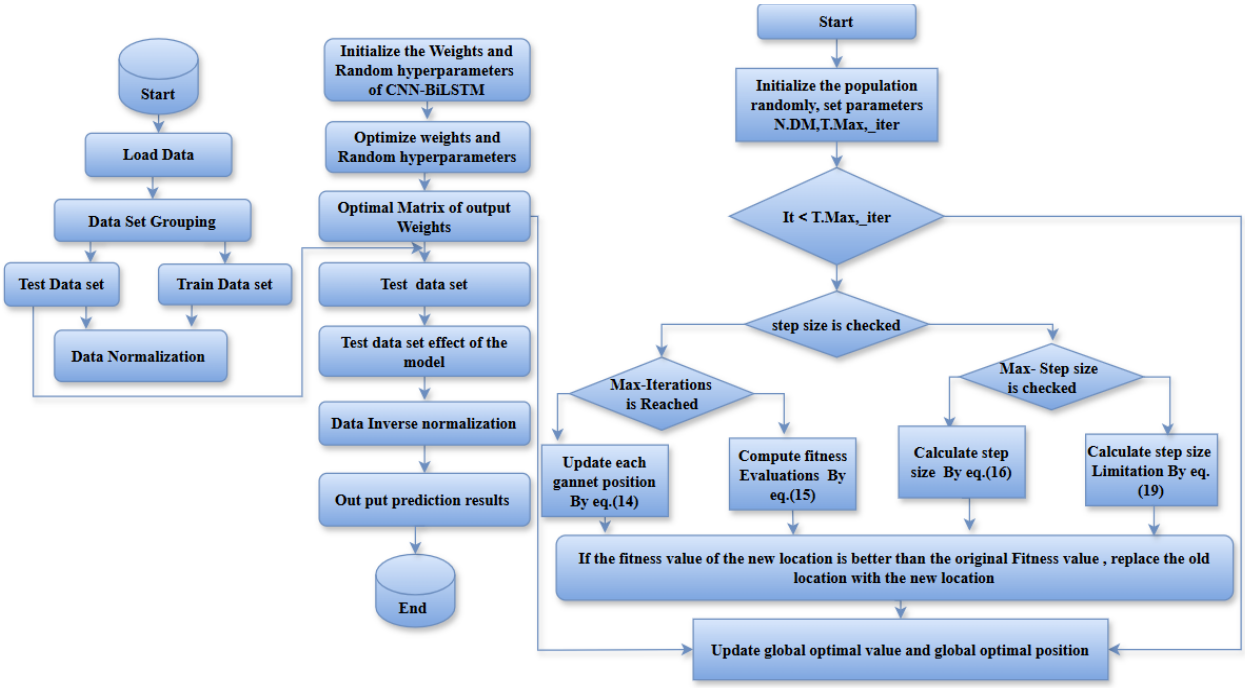

Figure 4. Flow chart for Proposed CNN-BiLSTM+ EGSO Techniques

Phase 1: Initialization with oppositional

To provide the best and global search results, this method uses the quasi opposition function [39]. This algorithm begins the search process with two arbitrarily generated objects in the search space that are connected to the following

$$O_i = LB_i + RAND\,.(UB_i - LB_i); i = 1,2,3,\dots n \quad (13)$$

$$x_i^{Q0} = RAND\left(\frac{LB_i - UB_i}{2}, LB - x_i\right), i = 1,2,3\dots pop \quad (14)$$

Here, $UB_i\ and\ LB_i$ is defined as lower and upper bounds. The position of the objects within the search space is denoted by O_i and Solution based on quasi-oppositional functions is denoted by x_i^{Q0}.

Phase 2: Fitness Computation

This step involves computing the starting population in relation tope objective function and selecting the object with the best fitness value. The fitness function is used to train and validate the suggested model. The low parameters of the utility function show how well the model's predictions for facial remarks matched reality. The fitness function therefore calculates the forecast accuracy. A Mean Square Error is how the fitness function is regarded.

$$FF = \frac{1}{N}\sum_{i=1}^{N}(t_i - p_i)^2 \quad (15)$$

Here, the total number of features is N. p_i is the definition of the expected parameters and the true parameters are represented by t_i.

Phase 3: Golden variation

The third stage involves sorting the items according to their fitness function and changing the object with the lowest fitness using a random solution.

Phase 4: Step size computation

The step size operator is taken into consideration in each iteration of the optimization process to modify the objects to the ideal solution. There are three components to the step size operator. In the first part, the transformer operator that reduces iteratively to balance the algorithm's local and global search estimated the previous variable of the step size, which is different. The distance between the object's current location and its best position to date was determined in this Trion by calculating the cosine of a random parameter with a range of 0 to 1. In the final part, the sine of a random parameter between d and 1 is multiplied to determine the distance between the current position of the ith object and the ideal position so far attained among all objects. The step size operator is generated at random in the first optimization iteration and updated using the following equations as needed.

$$S_{Ti}(T+1) = t.S_{Ti}(T) + C_1.Cos(R_1).(Obest_i - x_i(t) + C_1.Cos(R_2).\left(Obest_i - x_i(t)\right)) \quad (16)$$

Here, t is a transfer operator that changes the focus of search from exploitation to exploration. $Obest_i$ is described as the object's ideal final location. The random numbers in the range of (0,1) are designated as R_2 and R_1. The random numbers between 0 and 1 are designated as C1 and C2. The search performance is improved by this transfer operator, which also manages the ratio of local search in subsequent iterations to global search in initial iterations. Typically, this transfer function is decreasing and can be calculated with the following formula:

$$T = 100X(-20X\frac{T}{T_{Max}}) \quad (17)$$

Here, the maximum number of iterations is denoted by T_{Max}.

Phase 5: Step size limitation

Every iteration of the method works by controlling the distance that each object travels in each dimension problem. The objects can handle wider cycles in the issue space thanks to this stochastic variable step size. A necessary gap is designed to object clamp movement associated to, in order to prevent these oscillations and to lessen divergence and explosion.

$$-S_{TMax} \leq S_{Ti} \leq S_{TMax} \quad (18)$$

Here, S_{TMax} is a defined maximum movement produced that characterises the maximum variation of an item throughout an iteration while taking positional coordinates into account. The formulation of this process is as follows:

$$S_{TMax} = 0.1X(UB_i - LB_i) \quad (19)$$

Phase 6: Position updating

During this stage, the item travels to the global optimum in the search space associated with the equation below.

$$O_i(\mathrm{T}+1)=O_i(\mathrm{T})+S_{Ti}(T+1) \quad (20)$$

Phase 7: Termination Condition

This stage involves verifying the termination condition. Convergence occurs when the maximum number of iterations is reached. Ultimately, the best options are stored and taken into account in order to recognize face expressions.

4.Results and Analysis

This paper evaluate the proposed framework on large-scale financial datasets such as the IEEE-CIS Fraud Detection Dataset, the PaySim Mobile Financial Transactions Dataset, through experiments, Proposed CNN-BiLSTM-EGSA has been proven to yield better performance results compared with normal models like OCNN-RNN, Random Forest, XGBoost, SVM, LSTM.

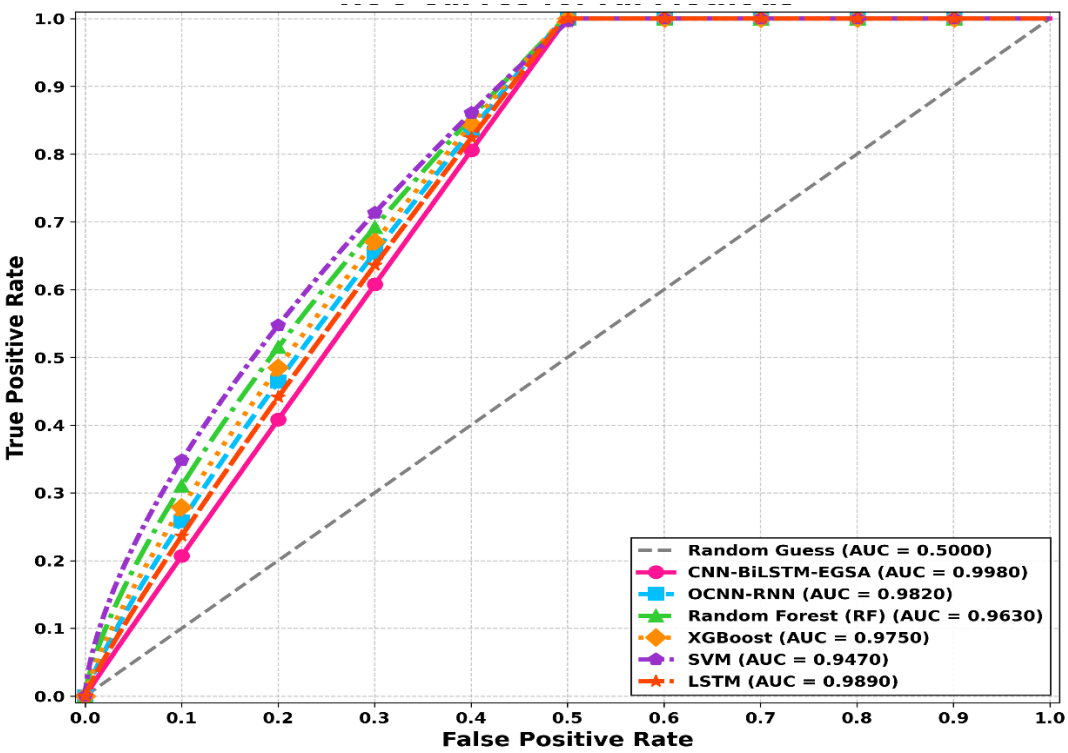

Figure 5. Roc curve with comparison all methods

As shown in Figure 5, the Receiver Operating Characteristic Curve In the ROC curve, the rate of false positive comparisons is compared with the rate of true positive comparisons. The paper assesses CNN-BiLSTM-EGSA, OCNN-RNN, RF, XGBoost, SVM, and LSTM. As FPR increases, TPR increases, indicating better detection of fraud. CNN-BiLSTM-EGSA captures a good TPR at low FPR, achieving at least 0.0216 (at FPR 0.01) and 0.408 (at FPR 0.2), thus striking the right TPR-FPR balance. OCNN-RNN stands next with 0.0366 (0.01) and 0.464(0.2). The RF and XGBoost do competitively attain 0.0578 and 0.0441 at FPR 0.01, and 0.5149 and 0.4845 at FPR 0.2, respectively. SVM & LSTM show a low recall at the beginning (0.0773 for SVM and 0.0297 for LSTM (FPR 0.01)), but turn to higher at FPR 0.2 (0.5474 for SVM and 0.4411 for LSTM).For false positive rate (FPR) values beyond 0.5, most models achieve a true positive rate (TPR) close to the value 1, meaning that those models capture almost all the fraud cases, but at the cost of more false positive predictions. It can be observed that generally CNN-BiLSTM-EGSA outperforms the rest of the classifiers with a good compromise between the high recall and the low FPR, whilst the RF and XGBoost also exhibit the potential. SVM and LSTM perform slightly worse but remain achievable at certain risks. This ROC analysis reinforces the requirement of performing fine-tuning on the models to enhance fraud detection.

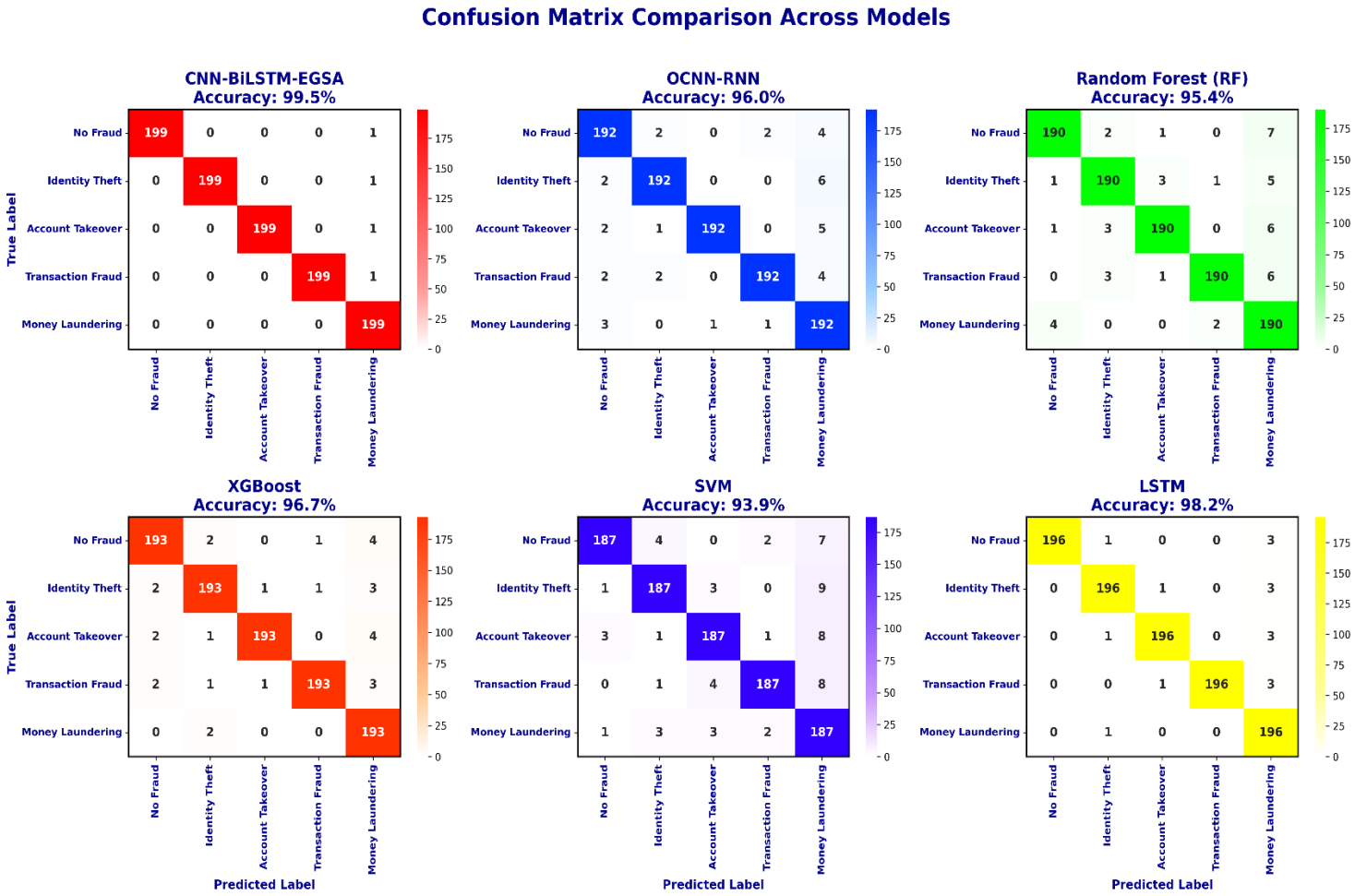

Figure 6. Confusion metrics with comparison all methods

As shown in Figure 6, the confusion matrix is used to describe the count of all labels correctly predicted by various fraud detection algorithms for each fraud category ,all models analysed in this paper (proposed method CNN-BiLSTM-EGSA, OCNN-RNN, RF, XGBoost, SVM, and LSTM) and the rows corresponding to the number of correctly classified transactions in each fraud type.CNN-BiLSTM-EGSA achieved the best perfect classification for all models, with 199 correctly predicted instances for each fraud type. This highlights its leading ability to detect no fraud, identity theft, account takeover, transaction fraud, and money laundering without false positives. Predictive results for LSTM and XGBoost were also significantly strong, correctly identifying 246 and 243 cases per class, respectively, indicating the effectiveness of these methods in classifying fraudulent patterns. However, SVM had fewer correctly classified counts 187 per fraud type, demonstrating poor output compared to deep learning-orientated models. OCNN-RNNcorrect predictions by class: 192 and Random Forest correct predictions by class: 190 achieved lower accuracy results, probably because these models could not model the complex sequential patterns of fraud as well as the hybrid deep learning models. Proposed CNN-BiLSTM-EGSA obtained such high accuracy because its CNN layers are useful for feature extraction, while BiLSTM is a good fit for capturing sequential dependencies in a financial transaction. Multiclass fraud detection performance confirms that CNN-BiLSTM-EGSA outperforms traditional models and other deep learning techniques, making it the most suitable approach for a multiclass fraud detection forecaster.

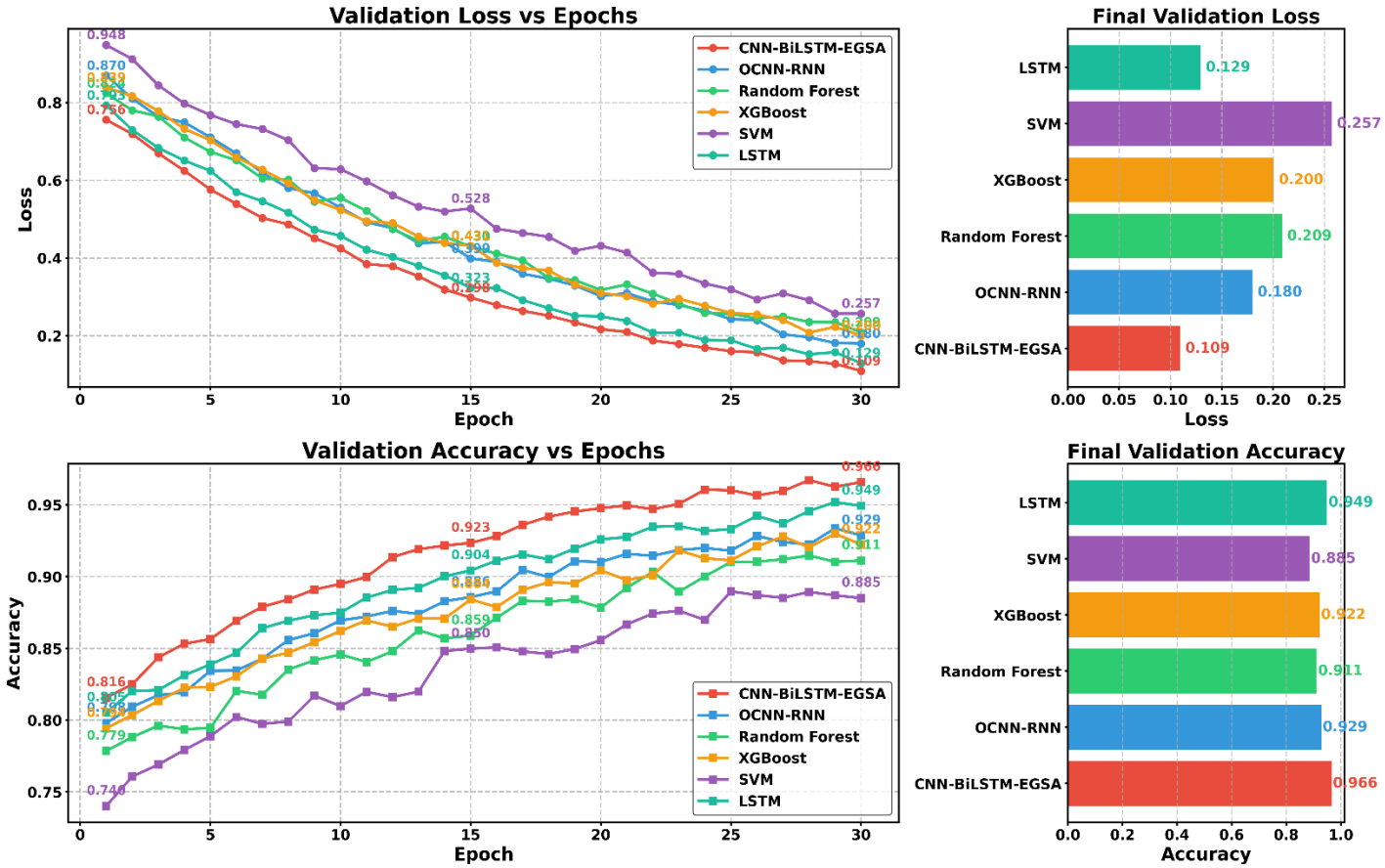

Figure 7. Performance of Validation loss and accuracy with comparison methods

As shown in figure 7. Performance of Validation loss and accuracy can serve as key indicators for the generalization performance of various fraud detection models. A lower validation loss means that the model is better optimized, whereas a higher validation accuracy means that it predicts better on unseen data. Among all the models, CNN-BiLSTM-EGSA is the best performing one, in which the validation loss and validation accuracy are 0.1092 and 96.59%, respectively. This implies that the model does a good job of being able to generalize to new instances of fraud, with very few false positives. The combination of CNN for feature extraction, BiLSTM for temporal pattern learning, and EGSA for hyperparameter tuning resulting in significant enhancement in the all-round fraudulent transactions detection. The LSTM worked well and completed with a validation loss of 0.1292 and an accuracy of 94.93% which further reflects that LSTM is suitable to work on sequential transaction data. But without CNN-based feature extraction, it is a little less effective than CNN-BiLSTM-EGSA.The Random Forest and XGBoost traditional machine learning models achieved a 91.12% and 92.24% validation accuracy, respectively, but at a relatively higher loss of (0.2085 and 0.2003). While featuring the ability of fraud detection through the generation of sequential patterns, these models are limited by the absence of deep analysis provided by BiLSTM architectures. The OCNN-RNN model showed moderate performance with a validation accuracy of 92.87% and a loss of 0.1797. Conversely, SVM demonstrated the least accuracy (88.50%) with the highest validation loss (0.2569), showcasing its insensitivity to fraud patterns embedded in complex financial transactions. Our findings support that CNN-BiLSTM-EGSA is the best performing architecture for multi-class financial fraud detection as it achieves the lowest validation loss and the highest validation accuracy. As a result, it can generalize better compared to other fraud types, making it an appropriate candidate for realistic, online paid fraud detection systems.

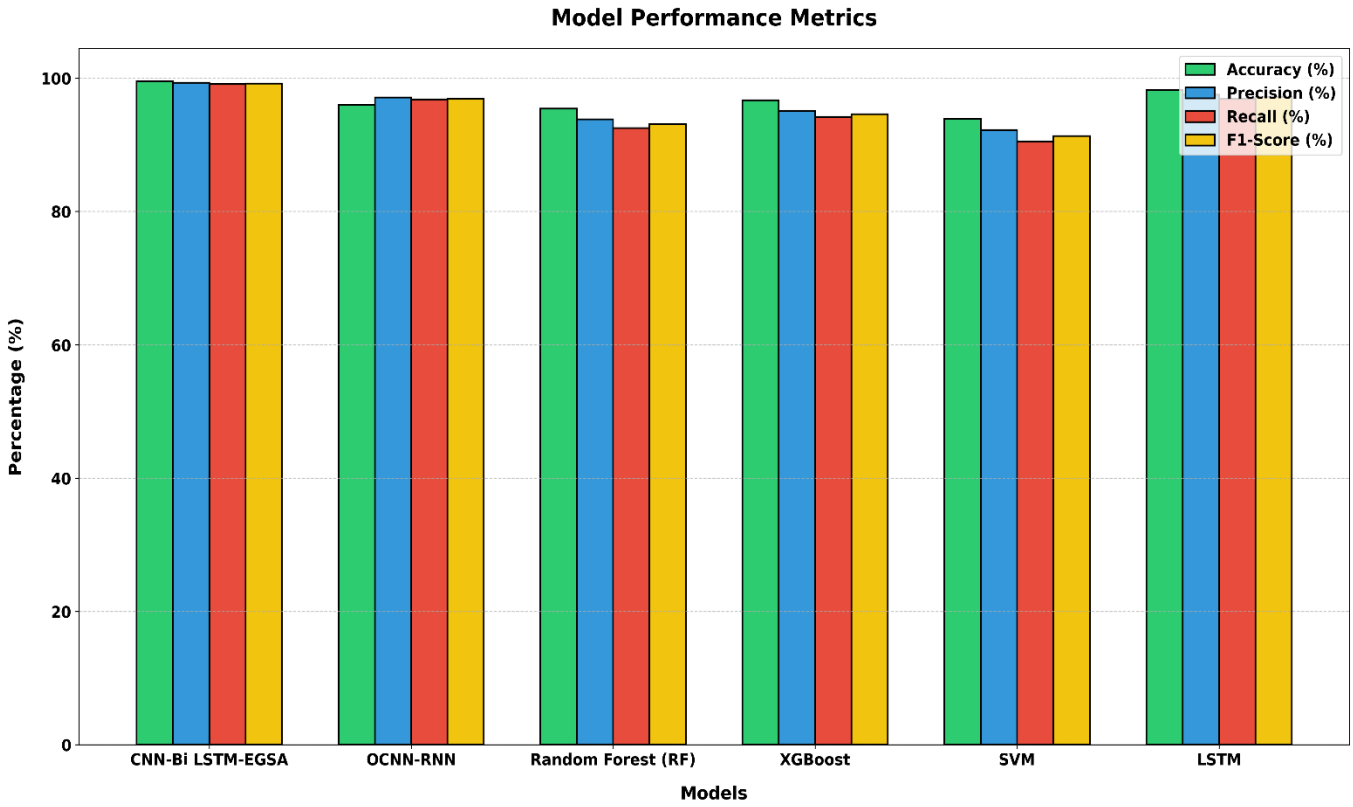

Figure 8. Performance metrics with comparison methods

As shown in Figure 8. Financial fraud detection models are evaluated based on accuracy, precision, recall, and F1 Score. The proposed CNN-BiLSTM-EGSA yields 99.5% accuracy, 99.3% precision, 99.1% recall, and a 99.2% F1 score, outperforming the other models. This indicates that it can detect fraud more accurately and with fewer false positives. OCNN-RNN comes next with an accuracy of 96.0% and an F1 score of 96.9%, indicating that this model performs rather balanced across classes. While XGBoost shows outstanding precision (95.1%) and recall (94.2%), Random Forest (RF) demonstrates good classification with 93.8% precision and 92.5% recall. Test performance (accuracy) of XGBoost is 96.7%. Conversely, SVM indicated a more conservative approach by having the least accuracy (93.9%) and recall (90. 5%).This data set provides competitive fraud detection performance of LSTM with 98.2% accuracy and a 97.2% F1 score. Overall, CNN-BiLSTM-EGSA performs best in every component, whereas RF and XGBoost provide powerful contenders. Finally, SVM sacrifices recall for precision, and LSTM achieves low detection efficiency. These findings underscore that the choice of a model depends on an organization's fraud prevention priorities and tolerance for business risk.

Figure 9 illustrates the outcomes. Using selectivity, specificity, and G-Mean fraudulent circumstances while minimizing false positives, more research on financial fraud detection techniques. With 99.2% selectivity, 99.3% specificity, and a G-Mean of 99.4%, CNN-BiLSTM-EGSA efficiently detects fraud, keeping a balanced false positive and false negative rate. With a G-Mean of 97.0%, OCNN-RNN shows strong resilience but somewhat less than CNN-BiLSTM-EGSA in capturing 96.5% selectivity and 96.7% specificity. Among the conventional machine-learning models, XGBoost (94.0% selectivity, 94.3% specificity, 94.5% G-Mean) and Random Forest (92.7% selectivity, 93.2% specificity, 93.0% G-Mean) both perform competitively; the former slightly outperforms the latter in total classification balance. A combination of the lowest selectivity (90.8%) and specificity (91.2%), SVM produces a 91.0% G-Mean, consequently indicating a more cautious classification method. LSTM detects fraud with a balanced misclassification rate having 96.8% selectivity, 97.0% specificity, and a 97.0% G-Mean. CNN-BiLSTM-EGSA is the most reliable metric-wise; LSTM and OCNN-RNN are strong substitutes. XGBoost and RF perform well; SVM trades recall for accuracy. These realisations guide the selection of the most appropriate fraud detection system depending on corporate risk tolerance**.**

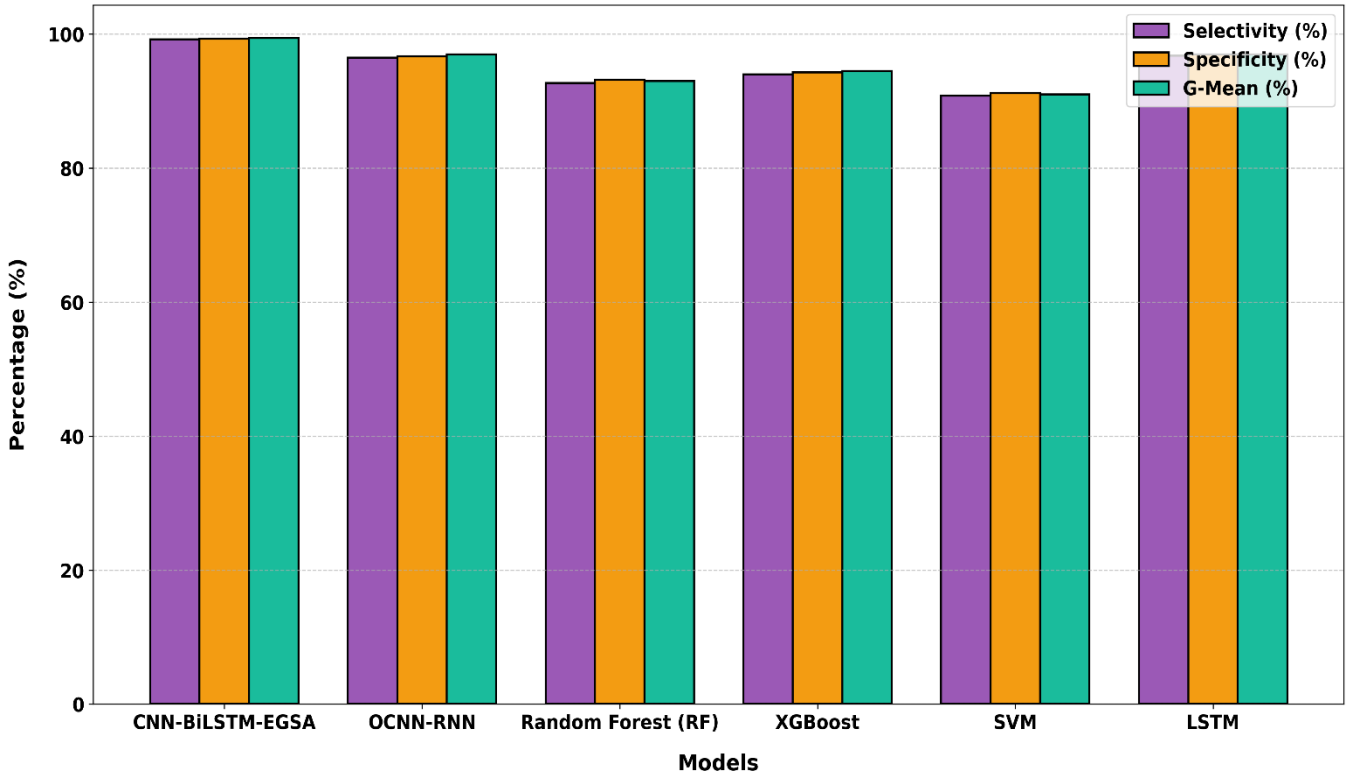

Figure 9. Performance metrics (selectivity, specificity, and G-Mean) with comparison methods

Figure 10 illustrates the outcomes.Matthews Correlation Coefficient (MCC) and Kappa let one assess the accuracy and consensus of models for fraud detection. With the best MCC (0.98) and Kappa (0.98), CNN-BiLSTM-EGSA demonstrates fraud classification accuracy. Furthermore, doing well are LSTM (0.96, 0.96) and OCNN-RNN (0.94, 0.94). While SVM (0.85, 0.85) has lower classification consistency, XGBoost (0.91, 0.91) and Random Forest (0.88, 0.88) challenge.

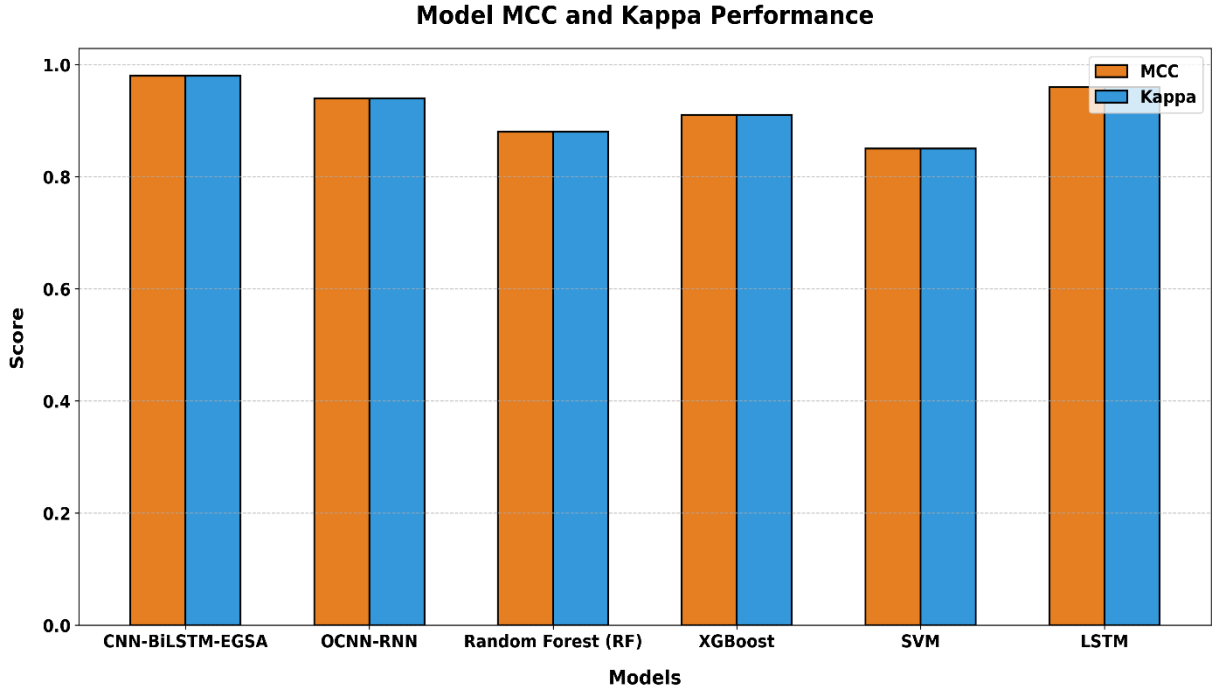

Figure 10. Performance metrics (MCC) and Kappa) with comparison methods

5.Conclusion

The changing character of fraudulent actions and the imbalance in transaction datasets make financial fraud detection still a major difficulty. By combining convolutional feature extraction, bidirectional sequential learning, and optimal hyperparameter tuning, the proposed Optimized Multi-Class Financial Fraud Detection Framework that incorporates Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM), whereas the Enhanced Golden Search Algorithm (EGSA) is utilized for

hyperparameter adjustment and feature optimization. The integrated CNN-BiLSTM drilling method to extract the spatial-temporal features further improves fraud detection in high-dimensional transactions While BiLSTM captures the sequential dependencies in financial transactions, the CNN layers lead to computationally efficient extraction of spatial correlations in the features of transactions. EGSA also tunes hyperparameters for better model training and achieves better performance of the method. According to the performance comparison method, such as proposed method CNN-BiLSTM-EGSA outperforms the traditional methods, for instance, OCNN-RNN, Random Forest, XGBoost, and Support Vector Machine (SVM), and standalone LSTM by correctly detecting fraudulent transactions in numbers of assessment criteria such as accuracy (99.5%), precision (99.3%), recall (99.1%), F1score (99.2%), AUC-ROC (99.8%), MCC (98%), G-Mean (99.4%), selectivity (99.2%), specificity (99.3%), and Kappa (0.98). The model largely solves many usage problems in terms of financial fraud detection, including class imbalance, feature selection, and computational efficiency.

Future Work

New Challenges Despite these positive findings, several limitations and directions for future work remain. The above-discussed CNN-BiLSTM-EGSA framework, when integrated with a block chain system (for example, the aforementioned CNN-BiLSTM-EGSA framework can monitor not merely transaction data but also customer-generated data such as social media and Internet activities, detected trade-line creation, etc., and further bridge that with block chain categorization) assists this integration in designing block chain-based monetary systems to improve secure transaction systems while enabling real-time accounting tracking for fraud detection. Moreover, the application of Explainable Artificial Intelligence (XAI) methods like SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) that are designed to improve the interpretability and explain ability of fraud detection models will give financial analysts a better understanding for striking fraudulent transaction predictions. Another aspect we need to consider is the notion of adversarial robustness: the fact that fraudsters will try to change and adapt their strategies so that they can no longer be detected. This can enhance the model's capacity to recognize counterfeit data, despite the existence of adversarial samples, by building defenses against such tactics. Similarly, federated learning is a new paradigm aimed at improving privacy-preserving fraud detection by allowing multiple financial institutions to collaboratively train models without revealing sensitive transaction information. This method means no organization has to share its sensitive data with other organizations, giving data security while enhancing fraud detection across the board. Through edge computing, the model can be deployed within edge devices, enabling real-time fraud detection by minimizing latency and increasing response times for the banking aspects. It will help the financial institutions to detect and avoid fraud on a real-time basis, which may lower the financial loss. Lastly, the diversification of the application of the model to other financial sectors (mechanism-based) is a great opportunity to improve its applicability and impact. In the future, work could be done to improve the architecture in these areas and make the CNN-BiLSTM-EGSA model more efficient, scalable, and reliable. This would create a safe and secure platform for financial transactions around the world.

Author contributions:
All the authors have equally contributed to preparing
the manuscript.
Availability of meta data and material
Not applicable
Funding
Not Applicable funding sources
Ethical approval
Not applicable
Consent to participate
Not applicable.
Consent to publish
Not applicable.
Data Availability
No Data Availability
Coding Availability

No Data Availability

Conflict of interest statement

I (we) certify that there is no conflict of interest with any financial organization regarding the material discussed in the manuscript.

Acknowledgements

Authors would like to thank the anonymous reviewers for their useful comments and suggestions

Reference

[1] H.R. Ranganatha, A Syed Mustafa, Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and blockchaintechnologies, *Expert Systems with Applications*, Volume 260,2025,125179, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2024.125179.

[2] Al-dahasi, E. M., Alsheikh, R. K., Khan, F. A., & Jeon, G. (2025). Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation. *Expert Systems*, 42(2), e13682. https://doi.org/10.1111/exsy.13682

[3] Pahuja, L., & Kamal, A. (2023). EnLEFD-DM: Ensemble Learning based Ethereum Fraud Detection using CRISP-DM framework. *Expert Systems*, 40(9), e13379. https://doi.org/10.1111/exsy.13379

[4] Cheng, D., Zou, Y., Xiang, S. *et al.* Graph neural networks for financial fraud detection: a review. *Front. Comput. Sci.* 19, 199609 (2025). https://doi.org/10.1007/s11704-024-40474-y

[5] Innan, N., Sawaika, A., Dhor, A. *et al.* Financial fraud detection using quantum graph neural networks. *Quantum Mach. Intell.* 6, 7 (2024). https://doi.org/10.1007/s42484-024-00143-6

[6] Gandhar, A., Gupta, K., Pandey, A.K. *et al.* Fraud Detection Using Machine Learning and Deep Learning. *SN COMPUT. SCI.* 5, 453 (2024). https://doi.org/10.1007/s42979-024-02772-x

[7] Zioviris, G., Kolomvatsos, K. &Stamoulis, G. An intelligent sequential fraud detection model based on deep learning. *J Supercomput* 80, 14824–14847 (2024). https://doi.org/10.1007/s11227-024-06030-y

[8] Vashistha, A., Tiwari, A.K. Building Resilience in Banking Against Fraud with Hyper Ensemble Machine Learning and Anomaly Detection Strategies. *SN COMPUT. SCI.* 5, 556 (2024). https://doi.org/10.1007/s42979-024-02854-w

[9] Chen, Y., Du, M. Financial Fraud Transaction Prediction Approach Based on Global Enhanced GCN and Bidirectional LSTM. *Comput Econ* (2024). https://doi.org/10.1007/s10614-024-10791-2

[10] Al-Sayyed, R., Alhenawi, E., Alazzam, H. *et al.* Mobile money fraud detection using data analysis and visualization techniques. *Multimed Tools Appl* 83, 17093–17108 (2024). https://doi.org/10.1007/s11042-023-16068-4

[11] Devaguptam, S., Gorti, S.S., Akshaya, T.L. *et al.* Automated Health Insurance Processing Framework with Intelligent Fraud Detection, Risk Classification and Premium Prediction. *SN COMPUT. SCI.* 5, 450 (2024). https://doi.org/10.1007/s42979-024-02801-9

[12] Gorle, V.L.N., Panigrahi, S. A semi-supervised Anti-Fraud model based on integrated XGBoost and BiGRU with self-attention network: an application to internet loan fraud detection. *Multimed Tools Appl* 83, 56939–56964 (2024). https://doi.org/10.1007/s11042-023-17681-z

[13] S. Patel, M. Pandey and R. D, "Fraud Detection in Financial Transactions: A Machine Learning Approach," *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, 2024, pp. 1-8, doi: 10.1109/ICONSTEM60960.2024.10568903.

[14] Kesharwani and P. Shukla, "FFDM-GNN: A Financial Fraud Detection Model using Graph Neural Network," *2024 International Conference on Computing, Sciences and Communications (ICCSC)*, Ghaziabad, India, 2024, pp. 1-6,

[15] Wang, M. Wang, X. Wang, L. Zhang and Y. Long, "Multi-Relational Graph Representation Learning for Financial Statement Fraud Detection," in *Big Data Mining and Analytics*, vol. 7, no. 3, pp. 920-941, September 2024, doi: 10.26599/BDMA.2024.9020013.

[16] Zhongzhen Yan, Hao Chen, Xinhua Dong, Kewei Zhou, Zhigang Xu, Research on prediction of multi-class theft crimes by an optimized decomposition and fusion method based on XGBoost, *Expert*

Systems with Applications, Volume 207,2022,117943, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2022.117943.

[17] Tragouda, M., Doumpos, M., & Zopounidis, C. (2024). Identification of fraudulent financial statements through a multi-label classification approach. *Intelligent Systems in Accounting, Finance and Management*, 31(2), e1564. https://doi.org/10.1002/isaf.1564

[18] Al-dahasi, E. M., Alsheikh, R. K., Khan, F. A., & Jeon, G. (2025). Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation. *Expert Systems*, 42(2), e13682. https://doi.org/10.1111/exsy.13682

[19] Singh, Ajeet, Jain, Anurag, Biable, SeblewongelEsseynew, Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine, *Applied Computational Intelligence and Soft Computing*, 2022, 1468015, 10 pages, 2022. https://doi.org/10.1155/2022/1468015

[20] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," in *IEEE Access*, vol. 11, pp. 137188-137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[21] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," in *IEEE Access*, vol. 8, pp. 25579-25587, 2020, doi: 10.1109/ACCESS.2020.2971354.

[22] Prabhakaran, N., Nedunchelian, R., Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection, *Computational Intelligence and Neuroscience*, 2023, 2693022, 13 pages, 2023. https://doi.org/10.1155/2023/2693022

[23] NaoufalRtayli, NourddineEnneya, Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization, *Journal of Information Security and Applications*, Volume 55,2020,102596, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102596.

[24] Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A Financial Fraud Detection Model Based on LSTM Deep Learning Technique. *Journal of Applied Security Research*, 15(4), 498–516. Alghofaili, Y https://doi.org/10.1080/19361610.2020.1815491

[25] M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review," in *IEEE Access*, vol. 10, pp. 72504-72525, 2022, doi: 10.1109/ACCESS.2021.3096799.

[26] H. Wang, W. Wang, Y. Liu and B. Alidaee, "Integrating Machine Learning Algorithms with Quantum Annealing Solvers for Online Fraud Detection," in *IEEE Access*, vol. 10, pp. 75908-75917, 2022, doi: 10.1109/ACCESS.2022.3190897.

[27] Y. W. Bhowte, A. Roy, K. B. Raj, M. Sharma, K. Devi and P. LathaSoundarraj, "Advanced Fraud Detection Using Machine Learning Techniques in Accounting and Finance Sector," *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICONSTEM60960.2024.10568756.

[28] Alsuwailem, A.A.S., Salem, E. &Saudagar, A.K.J. Performance of Different Machine Learning Algorithms in Detecting Financial Fraud. *Comput Econ* 62, 1631–1667 (2023). https://doi.org/10.1007/s10614-022-10314-x

[29] W. Xiuguo and D. Shengyong, "An Analysis on Financial Statement Fraud Detection for Chinese Listed Companies Using Deep Learning," in *IEEE Access*, vol. 10, pp. 22516-22532, 2022, doi: 10.1109/ACCESS.2022.3153478.

[30] N. Damanik and C. -M. Liu, "Advanced Fraud Detection: Leveraging K-SMOTEENN and Stacking Ensemble to Tackle Data Imbalance and Extract Insights," in *IEEE Access*, vol. 13, pp. 10356-10370, 2025, doi: 10.1109/ACCESS.2025. 3528079.

[31] Vanini, Paolo, Sebastiano Rossi, Ermin Zvizdic, and Thomas Domenig. "Online payment fraud: from anomaly detection to risk management." *Financial Innovation* 9, no. 1 (2023): 66.

[32] Abd El-Naby, Aya, Ezz El-Din Hemdan, and Ayman El-Sayed. "An efficient fraud detection framework with credit card imbalanced data in financial services." *Multimedia Tools and Applications* 82, no. 3 (2023): 4139-4160.

[33] Ni, Lina, Jufeng Li, Huixin Xu, Xiangbo Wang, and Jinquan Zhang. "Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection." *IEEE Transactions on Computational Social Systems* (2023).

[34] Agushaka, Jeffrey 0., Absalom E. Ezugwu, and LaithAbualigah. "Gazelle optimization algorithm: a novel nature-inspired metaheuristic optimizer." *Neural Computing and Applications* 35, no. 5 (2023): 4099-4131.

[35] Nour, Mohamed K., ImeneIssaoui, AlaaEdris, Ahmed Mahmud, Mohammed Assiri, and Sara Saadeldeen Ibrahim. "Computer Aided Cervical Cancer Diagnosis using Gazelle Optimization Algorithm with Deep Learning Model." *IEEE Access* (2024).

[36] Zhang, X., Ma, Y., & Wang, M. An attention-based Logistic-CNN-BiLSTM hybrid neural network for credit risk prediction of listed real estate enterprises. *Expert Systems*, 41(2), e13299,(2024). https://doi.org/10.1111/exsy.13299

[37] Noroozi, Mohammad, Hamed Mohammadi, EmadEfatinasab, Ali Lashgari, MandiyehEslami, and Baseem Khan. "Golden search optimization algorithm." *IEEE Access* 10 (2022): 37515-37532.

[38] Swami Nathan, Dhivya, Arul Rajagopalan, Oscar Danilo Montoya, Savitha Arul, and Luis Fernando Grisales-Norefia. "Distribution network reconfiguration based on hybrid golden flower algorithm for smart cities evolution." *Energies* 16, no. 5 (2023): 2454.

[39] Ahmad, Mohamad Faiz, Nor Ashidi Mat Isa, Wei Hong Lim, and Koon Meng Ang. "Differential evolution with modified initialization scheme using chaotic oppositional based learning strategy." *Alexandria Engineering Journal* 61, no. 12 (2022): 11835-11858.

[40] https://www.kaggle.com/competitions/ieee-fraud-detection

[41] https://www.kaggle.com/datasets/mtalaltariq/paysim-data