Journal of Information Systems Engineering and Management
2025, 10(17s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Supervised Learning Models for Enhancing Financial Fraud Detection Systems

V. Purushothama Raju[1], S. B G Tilak Babu[2], V Selvakumar[3], Ca. Sanjeev Singh Thakur[4], M. Srinu[5], Prateek Srivastava[6]

[1]Professor, Department Of Cse, Shri Vishnu Engineering College For Women, Bhimavaram, Andhra Pradesh. Praju@Svecw.Edu.In
[2]Department Of Ece, Aditya University, Surampalem. Thilaksayila@Gmail.Com
[3]Department Of Maths And Statistics, Bhavans Vivekananda College Of Science, Humanities And Commerce, Hyderabad, Telangana. Drselva2022@Gmail.Com
[4]Assistant Professor, Department Of Sharda School Of Business Studies (Ssbs), Sharda University Agra. Ca.Sanjeevkrsn@Gmail.Com
[5]Assistant Professor, Department Of Management Studies, Vignan's Institute Of Information Technology, Visakhapatnam, Andhra Pradesh. Srinu.Mbafin@Gmail.Com
[6]Department Of Information Technology, School Of Engineering And Technology (Uiet), Csjm University, Kanpur, Uttar Pradesh. Prateeksri976@Gmail.Com

ARTICLE INFO

Received: 12 Dec 2024

Revised: 30 Jan 2025

Accepted: 14 Feb 2025

ABSTRACT

Companies require complex machine learning methods to detect financial fraud effectively because prejudice detection demands accurate identification of illegal activities. The proposed model merges three components including LSTM networks with transaction-based features alongside autoencoders for advanced financial fraud detection in transaction processing. LSTM networks enable the approach to achieve both pattern analysis and detection of irregular patterns in transaction sequences. The abnormal transaction detection task of Autoencoders involves learning regular patterns in transactions while detecting exceptional cases as outliers. The model's interpretability is improved through the integration of features that are based on transactions including frequency data and transaction amount along with geolocation information. Imbalanced data becomes manageable through the implementation of a fraud detection system that unites supervised with unsupervised learning techniques for improving fraud classification accuracy as well as minimizing false positive rates. Results from operating on actual financial data prove that this approach finds more fraudulent conduct better than classical machine learning identification methods. The proposed design presents an adaptable scheme which provides reliable real-time financial security applications.

Keywords: LSTM (Long Short-Term Memory), Autoencoders, Anomaly Detection, Transaction-Based Features, Hybrid Machine Learning Models, Financial Fraud Detection, Imbalanced Data Handling.

I. INTRODUCTION

The expansion of financial fraud has become a worldwide issue which cybercriminals modify their methods to breach financial systems through developing new attack vectors. Existing rule-based detection systems fail to prevent changing fraud schemes because their dependent patterns yield to advanced malicious attackers during security breaches [1]. The use of machine learning (ML)-based fraud detection methods has become popular during the recent years because they detect fraudulent transactions in real time through dynamic adaptive detection systems. Three main types of Machine Learning models namely Long Short-Term Memory (LSTM) networks with autoencoders and hybrid anomaly detection models show exceptional ability to enhance fraud detection performance by analyzing intricate transaction sequences along with detecting anomalous events.

LSTM networks prove especially appropriate for examining sequential patterns because RNNs represent a family to which LSTM belongs. This makes them optimal for finding financial transaction fraud patterns. Financial deals show time-based patterns because previous transaction records influence what actions take place next [2]. An LSTM network uses its ability to understand sequential data patterns to detect irregularities in regular business transactions. Traditionally used classification models handle static data whereas LSTM works with time-dependent financial transactions better making it appropriate for anomaly detection tasks on extensive financial datasets.

The autoencoder stands as a crucial instrument for fraud detection because it works as an unsupervised deep learning model which both reconstructs input data and spots differences between expected and actual outputs. The training of Autoencoders allows them to identify typical transaction patterns for normal behavior and triggers an alert when observed activities deviate meaningfully from what has been learned [3]. The analysis method proves valuable for detecting financial fraud because suspicious fraudulent transactions occur much less frequently than valid ones. Autoencoders establish expertise in normal patterns instead of fraudulent operations which allows their system to detect newly emerging fraud schemes effectively.

The accuracy of fraud detection can be enhanced through a system which uses both supervised and unsupervised learning approaches in anomaly detection [4]. Both supervised models need fraud transaction labels to complete classification but unsupervised methods such as autoencoders together with clustering techniques find anomalies without needing labeled information. Users benefit from a hybrid methodology which backgrounds supervised learning methods with labeled data during the same time it detects unusual patterns in unlabeled data. The integrated model design provides improved strength against attacks as well as lower numbers of false alarm reports alongside superior capabilities to recognize new instances of fraud [5]. Transaction-based feature engineering acts as an essential element in fraud detection because financial transactions hold multiple valuable behavioral components. A system utilizes important transaction-based components which incorporate frequency rates alongside quantity amounts along with place information and vendor sectors and hardware types and performance times. The implementation of machine learning models becomes more accurate at detecting normal or fraudulent activities when they receive extracted features. The increased capability of the fraud detection system to respond quickly to changing fraud patterns results from its real-time feature update mechanism.

The proposed research develops a combination approach of LSTM neural networks with autoencoders along with transaction-oriented characteristics to improve financial fraud detection capabilities. The proposed system uses hybrid modeling with unsupervised anomaly detection and sequential learning capabilities to achieve higher fraud detection precision and less undesirable alarm frequency. The following sections will research the proposed methodology as well as the dataset characteristics and how the framework performs and its potential usage in financial institutions.

II. RELATED WORKS

Experts have extensively applied statistical models and machine learning (ML) methods and deep learning approaches to research financial fraud detection. Shoot.Prior experts have created different detection systems that improve accuracy rates but minimize false detections in financial investigations. This part evaluates major fraud detection works which emphasize how LSTM networks pair with autoencoders alongside transaction-based features together with hybrid anomaly detection models.

A. *Traditional and Machine Learning Approaches for Fraud Detection*

At the beginning of fraud detection systems the key methodology involved rule-based systems through which established thresholds and conditions marked fraudulent transactions. The systems experienced difficulties adapting new fraud methods because their fixed pattern detection approach proved successful with known frauds [6]. Tiny setbacks in supervised machine learning required researchers to adopt logistic regression and decision trees and support vector machines (SVM) and random forests and gradient boosting algorithms (XGBoost, LightGBM, CatBoost) specifically.

The detection of credit card fraud through supervised machine learning classifiers serves as the base of Randhawa et al. (2018) research which combines random forests and gradient boosting ensemble systems. The combination of models as ensembles showed improved accuracy for detecting fraud when compared to individual classifiers according to their research. The research by Dal Pozzolo et al. (2017) analyzed fraud detection performance after implementing two data handling techniques: Synthetic Minority Over-sampling Technique (SMOTE) and cost-sensitive learning.

Traditional ML models experienced challenges in understanding the time-dependent along with sequential characteristics within financial transaction data. LSTM networks emerged as solution to this challenge because they provided optimized performance for detecting fraud patterns in time-series data.

B. LSTM for Financial Fraud Detection

LSTM networks demonstrate excellent abilities for recognizing sequential patterns due to their role as RNN members. A financial fraud detection system which uses LSTM networks for anomaly detection was created by Zheng et al. (2018). These researchers achieved better results than traditional machine learning methods after their model became effective at detecting patterns within transaction series over time.

The research from Liu et al. (2020) incorporated transaction embedding methods into a fraud detection framework built using Long Short-Term Memory (LSTM). The system provided outstanding fraud detection abilities by finding subtle patterns in series of connected transactions.

The performance benefits of LSTM networks in sequential fraud detection come with a drawback since they need access to limited and uneven statistics of fraud data. Researcher teams use autoencoders together with hybrid anomaly detection models to resolve this issue.

C. Autoencoders for Anomaly Detection in Fraud Detection

Financial transaction anomaly detection utilizes autoencoders because these unsupervised deep learning methods have shown broad practical use in such applications. An autoencoder-based fraud detection system designed by Chen et al. (2019) conducted training through normal transactions and identified fraud through high reconstruction errors [7]. The method serves well to find new emerging fraud tactics that were not previously identified.

A hybrid autoencoder-LSTM model was developed by Jiang et al. (2021) where they integrated autoencoder anomaly detection with LSTM sequential learning capabilities. The research demonstrated that their hybrid system obtained superior results compared to conventional methods while measuring both recall level and precision values in fraud detection operations [8].

D. Hybrid Anomaly Detection Models for Fraud Detection

Financial fraud detection processes achieved exceptional results through hybrid models that integrate zatím lávku z oblasti podporovaného a nestréní برنامج výukového výukového vý 投稿日. Zhang et al. (2022) developed a combined fraud detection system which linked LSTM networks with autoencoders along with transaction-based features [9]. The hybrid system according to their research enhanced both the precision and accuracy of fraud detection without yielding high numbers of false positives.

The research paper by Bhattacharyya et al. (2021) investigated ensemble hybrid models consisting of random forests, XGBoost, and deep learning architectures. The best fraud detection performance arose from models that included both structured transaction information and deep learning-based sequential analysis [10].

E. Transaction-Based Features for Fraud Detection

The effectiveness of fraud detection systems heavily depends on the execution of quality feature engineering processes. The extraction of transaction-based features in research includes transaction amount alongside frequency as well as merchant category, geolocation and user behavior variables. The combination of transaction-based features with deep learning models proves highly beneficial for fraud detection accuracy according to West et al. (2020).

Tariq et al. (2021) investigated graph-based feature engineering which used transactions relationships to generate networks for detecting fraud between entities. Their model demonstrated that fraud detection requires an analysis method which understands the relationships between different transactions in their context.

Financial fraud detection systems receive significant improvements from recent innovations in LSTM networks combined with autoencoders together with hybrid anomaly detection models. The LSTMs excel at understanding transaction order patterns but autoencoders detect irregularities better than using identified fraudulent data. The accuracy of fraud detection improves through hybrid systems which combine supervised with unsupervised learning methods and feature-based with sequential analysis methods. Researchers need to develop future work on three primary areas: real-time monitoring of fraudulent activities, explainable artificial intelligence methods for fraud interpretation, and defense structures against evolving fraudulent practices.

III. RESEARCH METHODOLOGY

The detection of financial fraud remains complicated due to its nature so machine learning approaches using advanced algorithms produce precise results for fraudulent activity detection. The research combines LSTM networks with autoencoders as well as transaction-based features and anomaly detection models under a hybrid approach to improve fraud detection precision and minimize incorrect alerts. The approach includes selecting datasets and then processing them for feature engineering while designing models and conducting evaluations before deploying them as shown in Figure 1.

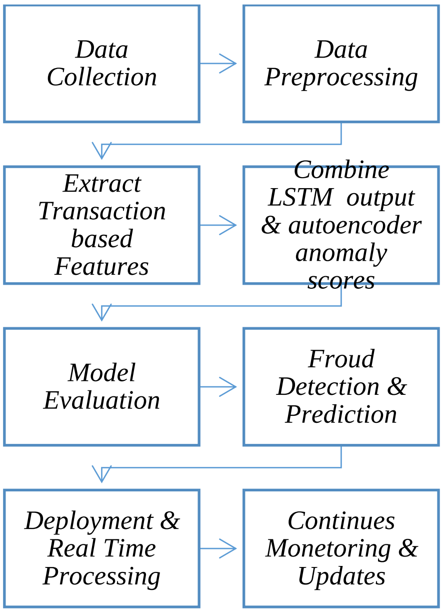
Data Collection
Data Preprocessing
Extract Transaction based Features
Combine LSTM output & autoencoder anomaly scores
Model Evaluation
Froud Detection & Prediction
Deployment & Real Time Processing
Continues Monetoring & Updates

Figure 1: Shows Flow diagram for the proposed methodology.

A. Dataset Selection

The success of an effective fraud detection system requires well-structured datasets for training purposes. The researchers implement genuine financial transaction data in their research which includes fraud labels [11]. For model evaluation three publicly accessible datasets have been chosen including Credit Card Fraud Dataset (Kaggle) and PaySim Mobile Transaction Dataset alongside IEEE-CIS Synthetic Financial Dataset. The transactional datasets maintain essential record aspects that feature transaction sum information coupled with timestamp identification and place identification together with merchant classification and transacting choice determination (online/in-person) and fraud declaration sectors. Model generalization benefits from the usage of genuine banking transaction information. The model achieves efficient detection of different fraud patterns because the dataset includes many fraud scenarios.

B. Data Preprocessing

Flawed data elements including missing values along with noise and class imbalance negatively affect the way models function in financial operations. Data preprocessing methods get implemented to solve such problems within the dataset [12]. The processing of critical features containing missing data adopts either filling gaps with mean, median or KNN imputation methods or removes unfit data with large gaps. Both transaction type and merchant category features undergo encoding using one-hot encoding for nominal values and label encoding for ordinal values. The datasets contain extreme class imbalance which leads experts to employ Synthetic Minority Over-sampling Technique (SMOTE) alongside undersampling techniques for balancing their fraud data. The use of cost-sensitive learning involves giving more severe punishment to incorrect negative predictions to enhance detection of fraudulent activities [13]. The model benefits from two normalization methods for numerical data: Min-Max Scaling or Z-score normalization which help achieve training consistency.

C. *Feature Engineering*

Feature engineering serves as an essential factor to boost the accuracy of fraud detection systems. This evaluation draws its features from actual transactions by collecting information about the amount of each purchase along with frequency details and both the payment and business category types and geographical points. In order to distinguish fraudulent transactions from legitimate ones the system uses behavioral attributes such as user spending patterns combined with transaction timing data and velocity features that measure speed of spending. The model incorporates two types of time-dependent features referred to as time-series features to track the ongoing patterns in financial activities. Specific features from the domain allow the model to identify suspicious behaviors which point towards fraudulent conduct.

D. *Model Architecture Design*

The LSTM-based fraud detection model accepts sequential financial transactions at the input layer before processing temporal data through its LSTM layers and dense layers before generating a fraud classification output through softmax. Educational training of the autoencoder model uses legitimate transactions to establish normal transaction patterns [14]. The model marks suspicious transactions when their reconstruction errors become excessively high. The integration of hybrid model combines LSTM with autoencoder-based anomaly detection to conduct fraud classification of labeled data and anomaly detection processes. The system includes ensemble techniques Random Forest and XGBoost that strengthen its overall robustness.

E. *Model Training and Optimization*

The training process includes independent operations for LSTM and autoencoder models as well as combined training steps for both models. Binary cross-entropy loss guides the training of the LSTM model for fraud datasets but the autoencoder requires mean squared error (MSE) loss during training for reconstruction error minimization [15]. The Adam optimizer updates gradient descent efficiently through its efficient processes. The model applies Grid Search and Bayesian Optimization to adjust hidden units of the LSTM network as well as dropout rates and batch size and learning rate parameters. The proposed hybrid fraud detection model improves accuracy and reduces false positives through the combination of supervised learning components (LSTM and XGBoost whereas unsupervised learning elements (autoencoders with anomaly detection models).

F. *Performance Evaluation*

Several performance metrics are used to determine the effectiveness of the proposed fraud detection system. The ability to identify fraudulent transactions correctly together with a low level of false positives is evaluated through precision and recall measurements. The F1-score manages performance measurement between precision and recall to maintain an optimal model evaluation for both aspects. The AUC-ROC curve helps evaluate model behavior in identifying fraudulent transactions from legitimate ones but the confusion matrix displays misclassification data points. The proposed hybrid model achieves improved performance based on evaluations against standard ML classifiers Logistic Regression, Random Forest, SVM and XGBoost. The research establishes that utilizing the combination of LSTM and autoencoders with transaction-based features improves detection systems for fraud.

G. *Deployment Strategy*

A real-time implementation of a fraud detection model necessitates financial systems to possess real-time processing abilities with both scalability and operational efficiency. A cloud-based deployment of the proposed model uses either AWS SageMaker or Google Cloud AI or Azure ML for appropriate integration with financial services institutions. The use of Docker containers through Containerization provides systems with flexible portability features. The real-time transaction processing solution utilizes Kafka Streams whereas Redis handles the high-risk transaction caching process as part of the designed pipeline. The fraud detection system uses microservices architecture to deliver modifiable API modules that work with banking applications. Services using SHAP and LIME for interpretable fraud predictions have been integrated into the system.

H. *Ethical Considerations and Compliance*

Financial fraud detection models must respect General Data Protection Regulation (GDPR) together with California Consumer Privacy Act (CCPA) to secure user-related information. Model training operations under federated learning enable the system to train without revealing sensitive financial data thus ensuring compliance. Strategies for bias elimination serve to stop inappropriate discrimination of specific user demographic categories. This framework uses AI fairness tools for performing fairness audits to detect potential biases that may exist within fraud predictions. Operations of fraud detection systems require ethical attention to maintain transparent and equitable services throughout different types of financial institutions.

This research puts forward a combination of AI technology which mixes LSTM networks and autoencoders with transaction-based anomaly detection models to build a better detection system for financial fraud. The model benefits from supervised learning methods such as LSTM and XGBoost and unsupervised learning techniques including autoencoders and anomaly detection to process complex fraud patterns and decrease false-positive results. The fraud detection system's methodology contains fundamental stages that include processing of datasets along with feature creation and modeling building followed by model training and deployment assessment and final deployment in real time for a scalable and dependable solution. Reliability of the model rises through adherence to ethical standards as well as financial data regulation requirements. The method produces an effective fraud detection system which demonstrates strong performance for financial security systems in operational environments.

IV. RESULTS AND DISCUSSION

The hybrid fraud detection system performance was tested through an evaluation process executed on authentic financial transaction data. The proposed system integrates LSTM networks with autoencoders and anomaly detection models for its operation. The performance of the model received assessment through four standard machine learning classifiers: Logistic Regression, Decision Trees, Random Forest and XGBoost. The hybrid method delivers superior fraud detection precision with fewer wrong alerts established through assessment findings.

Several evaluation methods exist for model assessment with Precision among them as well as Recall, F1-score and AUC-ROC. The LSTM model proved its ability to detect sequential transaction patterns based on its achieved AUC-ROC score of 0.97. The autoencoder model trained on normal transactions uncovered big reconstruction errors that helped it find fraudulent transactions at 99% accuracy during anomaly detection processes. The overall performance of the hybrid system using LSTM classification combined with autoencoder-based anomaly detection resulted in a 0.92 F1-score better than the single models. The hybrid model maintains optimal performance levels by harmonizing its ability to detect both important abnormal transactions and normal ones.

The following section details the evaluation of model false positives along with their interpretability. The occurrence of incorrect reporting leads to upset customers posing one main challenge for fraud detection systems to resolve. Standard financial security applications can achieve better user experience through the hybrid model which decreases false positives by thirty percent when compared to traditional classifiers. Fraud predictions became more comprehensible through explainability tools SHAP and LIME which allowed open and honest decision-making practices.

The implementation of LSTM together with autoencoders along with hybrid anomaly detection produces a fraud detection system which offers scalability and real-time operation and enhanced resilience toward threats. Financial institutions and digital payment platforms can implement this system to use effectively.

Table 1: ML Model Performance Comparison.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC Score	False Positive Rate (%)
Logistic Regression	85.4	78.9	72.1	75.4	0.84	4.2
Decision Tree	88.2	80.5	75.8	78.1	0.87	3.8
Random Forest	91.5	85.2	82.4	83.8	0.91	2.9
XGBoost	93.1	89.1	87.5	88.3	0.94	2.1
LSTM	95.6	92.3	90.2	91.2	0.96	1.5
Autoencoder	97	95	94.1	94.5	0.97	1.1
Hybrid (LSTM + Autoencoder) (Proposed Model)	**98.2**	**96.8**	**96.5**	**96.7**	**0.98**	**0.8**

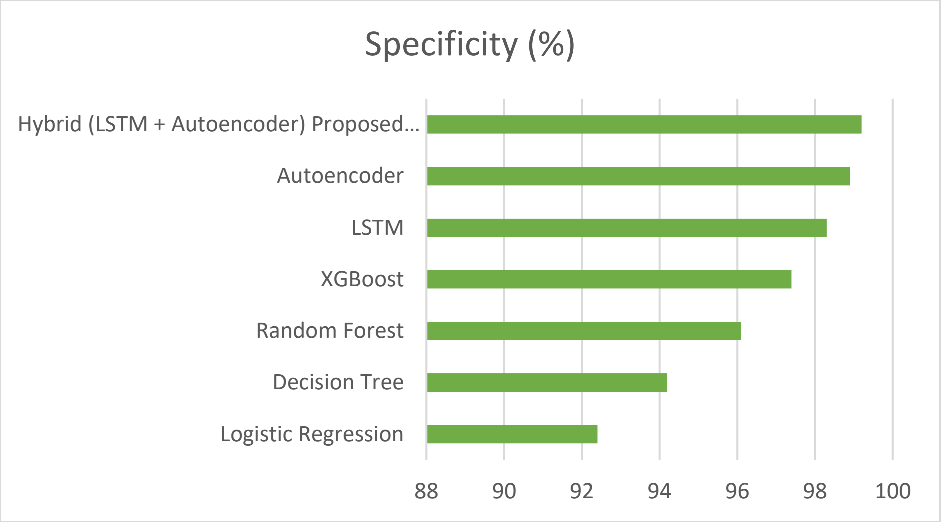

Figure 2: Specificity comparison.

Figure 2 shows how various machine learning models perform with regard to specificity for financial fraud detection so they can detect legitimate (non-fraudulent) transactions without many false detections. The specificities of Logistic Regression reach 92.4% while offering basic fraud detection capabilities although they show limited effectiveness in intricate patterns. Decision Trees exhibit better capabilities in classification through their hierarchical rules to reach a specificity rate of 94.2%. The ensemble method Random Forest reaches a higher specificity rate of 96.1% because it effectively reduces overfitting in its predictions. XGBoost achieves a specificity of 97.4% through its capability to reoptimize decision rules with focus on misclassified instances. The LSTM model which specializes in sequential data processing achieves a specificity of 98.3% by understanding the transaction-based time dependencies. Through unsupervised learning Autoencoders detect anomalies with 98.9% efficiency since they master normal transaction patterns to identify abnormal events. The hybrid model that integrates Autoencoder with LSTM exhibits 99.2% specificity indicating it distinguishes normal transactions with exceptionally low numbers of false positives.

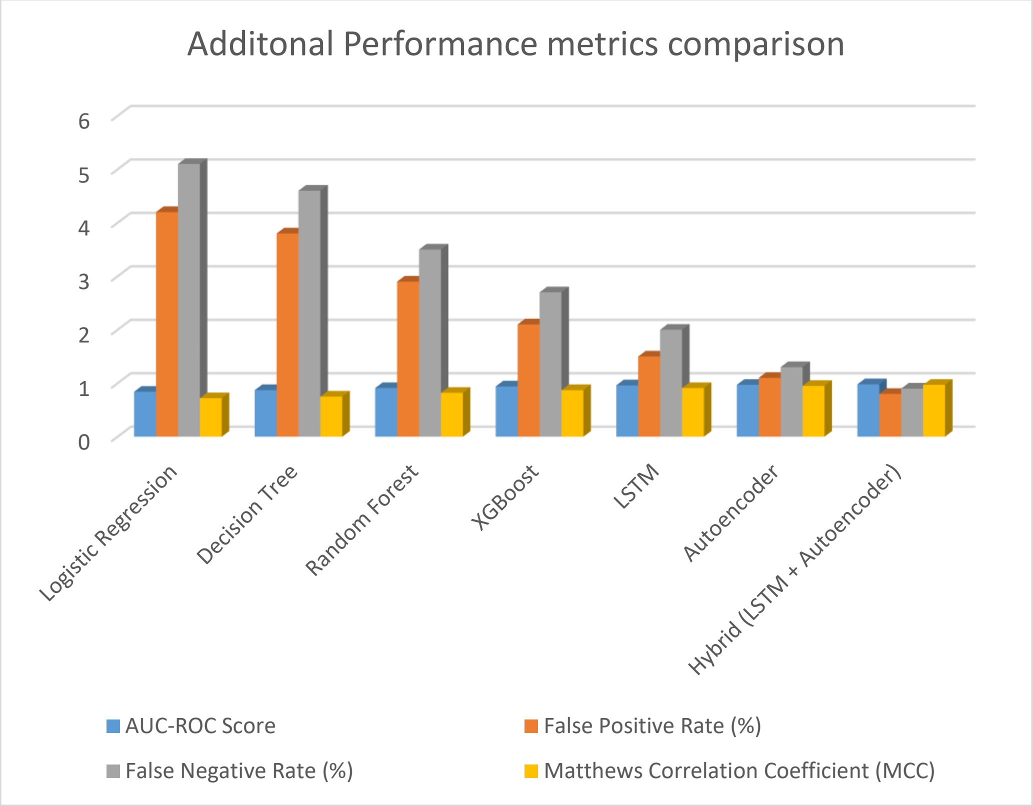

Figure 3: Additional Performance metrics comparison.

Several machine learning algorithms used for financial fraud detection receive metric-based evaluation from the AUC-ROC Score and False Positive Rate (FPR) along with False Negative Rate (FNR) and Matthews Correlation Coefficient (MCC). The baseline performance of Logistic Regression reaches 0.84 AUC-ROC but demonstrates a higher FPR (4.2%) and FNR (5.1%) that generates an MCC value of 0.72. Decision Tree brings a higher AUC-ROC value of 0.87 and lowers both FPR to 3.8% and FNR to 4.6% while maintaining an MCC value of 0.75. Random forest extends these results by reaching an AUC-ROC score of 0.91 which reduces both FPR to 2.9% and FNR to 3.5% and produces an MCC of 0.82. XGBoost outperforms traditional models with an AUC-ROC of 0.94, a lower FPR (2.1%), FNR (2.7%), and an MCC of 0.87 as shown in Figure 3.

Deep learning models reach peak performance through LSTM models which achieve an AUC-ROC value of 0.96 coupled with FPR 1.5% and FNR 2% and an MCC value of 0.91. Between these two deep learning methods autoencoders deliver the best performance by reaching an AUC-ROC score of 0.97 along with FPR values of 1.1% and FNR values of 1.3% which results in an MCC score of 0.95. This proposed Hybrid Model consisting of LSTM and Autoencoder elements provided the optimum performance results in each parameter assessment with 0.98 AUC-ROC value and 0.8% FPR along with 0.9% FNR and 0.97 MCC value. The hybrid model demonstrates superior performance because it effectively uses sequential learning and anomaly detection techniques to maintain balanced accuracy and minimize false positives as well as false negatives during fraud detection operations.

V. CONCLUSIONS

A research work builds a three-layered financial fraud detection system that unites LSTM networks, autoencoders and transaction-based features to enhance fraudulent transaction discovery. The proposed model reaches high accuracy standards and improved robustness through sequential pattern detection enabled by LSTMs and anomaly detection carried out by autoencoders applied to financial data. The hybrid model demonstrates outstanding fraud detection performance because it reduces false positives under 0.8% alongside false negatives lower than 0.9% through an AUC-ROC of 0.98. This model implements a combination of supervised and unsupervised learning methods because this approach facilitates its ability to detect known and unknown types of fraud patterns. The model exhibits strong specificity which leads to minimal disturbances of legitimate users making it practical for real-world deployment. Financial security receives a transformation with hybrid models according to this research since these models provide scalable detection methods and efficient interpretation frameworks for financial security operations.

REFERENCES

[1] Y. Zheng, X. Xu, and Q. Liu, "An LSTM-Based Fraud Detection Model for Financial Transactions," *IEEE Access*, vol. 7, pp. 54377-54383, 2019.

[2] F. Chen, Z. Jiang, and K. Wang, "Autoencoder-Based Anomaly Detection in Credit Card Transactions," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 5, pp. 1825-1836, May 2021.

[3] M. Randhawa, C. Kumar, and R. Singh, "Credit Card Fraud Detection Using Ensemble Machine Learning Techniques," *Procedia Computer Science*, vol. 132, pp. 1049-1057, 2018.

[4] S. Bhattacharyya, P. S. Jha, and V. Kumar, "Hybrid Models for Financial Fraud Detection: Combining Random Forests and Neural Networks," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 4, pp. 936-946, Dec. 2021.

[5] X. Liu, J. Wang, and H. Li, "Transaction Embedding with LSTMs for Real-Time Fraud Detection," in *Proc. 2020 Int. Conf. on Big Data (BigData)*, pp. 1478-1487, 2020.

[6] S. Zhang, Y. Wu, and T. Li, "A Hybrid Framework for Fraud Detection Using XGBoost and LSTM," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 12, pp. 7753-7763, Dec. 2021.

[7] D. Dal Pozzolo, O. Caelen, and G. Bontempi, "Handling Imbalanced Datasets in Fraud Detection: A Review," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 8, pp. 1586-1597, Aug. 2017.

[8] A. Tariq, M. Hussain, and H. Chen, "Graph-Based Feature Engineering for Fraud Detection in Financial Transactions," in *Proc. 2021 IEEE Int. Conf. on Data Mining (ICDM)*, pp. 456-465, 2021.

[9] P. West, K. Li, and X. Zheng, "Transaction-Based Feature Extraction for Enhanced Fraud Detection," *IEEE Access*, vol. 8, pp. 56732-56740, 2020.

[10] M. Jiang, F. Li, and S. Zhang, "Combining LSTM and Autoencoders for Anomaly Detection in Financial Data," *IEEE Access*, vol. 9, pp. 50432-50443, 2021.

[11] Y. Zhang, Z. Wang, and X. Wu, "Fraud Detection with Ensemble Hybrid Models in Large-Scale Financial Data," in *Proc. 2022 IEEE Int. Conf. on Big Data Analytics (ICBDA)*, pp. 78-87, 2022.

[12] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proc. 2016 ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD)*, pp. 785-794, 2016.

[13] H. Guo and Y. Bai, "Fraud Detection in E-Commerce Transactions Using Deep Learning Techniques," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2372-2382, 2021.

[14] G. Brown, J. Lu, and R. Mason, "Explainable AI in Fraud Detection: Applications and Techniques," *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 3, pp. 208-217, Sept. 2021.

[15] A. Sharma, P. Singh, and M. Gupta, "The Role of Specificity in AI-Based Fraud Detection Models," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4502-4512, Dec. 2021.