

Hybrid ML Framework for Financial Fraud Detection Using Statistical and DL Models

Himanshi Jain (Research Scholar), Prof. (Dr.) Parveen Sehgal (Supervisor)

Department of CSE, Om Sterling Global University, Hisar

Abstract: Fraud in the digital financial system is now a big challenge because of the rapid growth of online banking, e-commerce and online transactions. Fraud patterns are dynamic and continually evolving; it is very difficult to uncover fraud using traditional rule-based and simple statistical methods. To overcome this hurdle, in this study, an appropriate hybrid model of ML which uses the DL techniques with the statistical learning models are proposed, which would be effective in detecting financial fraud. The proposed method in this work is a fusion of several DL models (FNN, CNN, RNN) and the statistical models (Random Forest, Logistic Regression and Support Vector Machines) with their advantages. It is based on the pre-processing of data, feature extraction, model training, and evaluation of model performance. Experimental results showed that the hybrid model has achieved better detection accuracy than the conventional ML models. The proposed framework has the potential to significantly benefit banks, insurance companies and other financial institutions by reducing losses and enhancing the security of transactions.

Keywords: FFD, ML, DL, Hybrid Models, AI, Credit Card Fraud

1. INTRODUCTION

In today's digital economy, financial fraud against financial institutions, e-commerce platforms and digital payment systems has emerged as a core challenge [1]. In the past years online banking, mobile payments, cryptocurrency transactions, digital financial services, etc. have gained momentum, leading to a huge boost in financial transactions. These technologies advance access and efficiency but also open the door for scammers to take advantage of vulnerabilities in the systems. Adverse events like credit card fraud, identity theft, money laundering, insurance fraud and false financial statements cost big money and erode trust in financial systems [2].

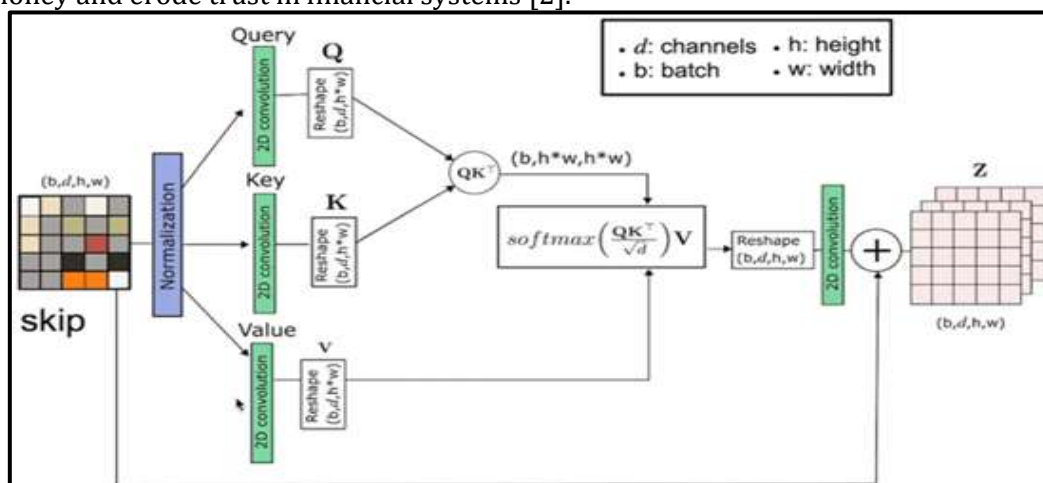


Figure 1: Financial Fraud Detection

The traditional fraud detection methods rely primarily on rule-based and statistical techniques. They are not effective or scalable to overcome ever-changing fraud patterns and tend to have high false positive rates. In response to these restrictions, financial institutions have been increasingly turning to AI, ML and DL techniques. In the context of ML, large datasets can be used to detect complex fraud patterns, using models like Decision Trees, Random Forest, SVM and Neural Networks [3]. But one model per individual might be inadequate for dealing with unbalanced information and fluctuating fraud patterns. Hence, hybrid systems (statistical analysis with ML and DL models) offer more accurate fraud detection, fewer false alarms and better known and unknown fraud detection capabilities.

1.1 Financial Fraud in the Digital Economy

Digitalization of financial services has revolutionized the global financial transaction system. Financial transactions are now faster, easier and more convenient with online banking, digital wallets, e-commerce platforms and mobile payment systems [4]. Fraudsters devise new and sophisticated methods for exploiting system vulnerabilities and outsmarting conventional fraud detection methods. There are many different types of financial frauds such as credit card fraud, account takeover fraud, identity theft fraud, insurance fraud, tax fraud, and money laundering. These fraudulent practices have severe monetary consequences and impact the credibility of financial organizations [5]. With the ever-growing digital financial landscape, the number of financial fraud cases globally is on the rise.

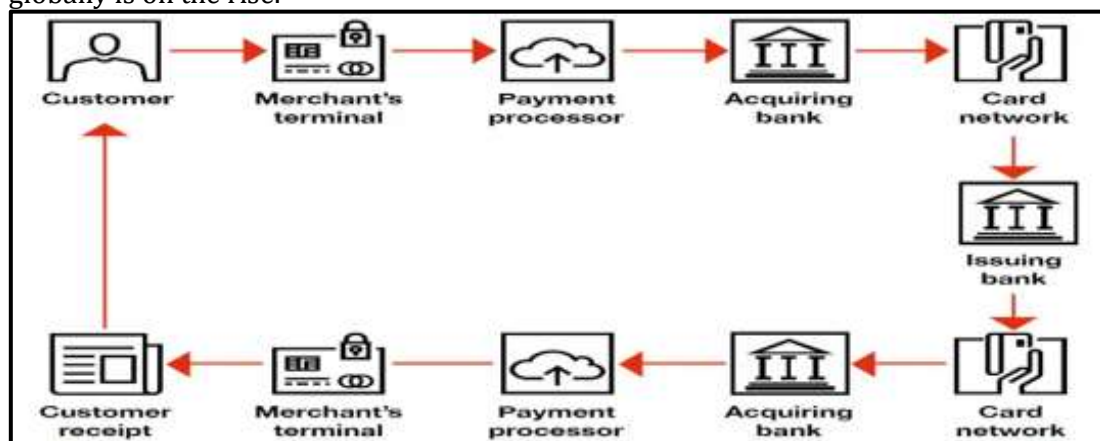


Figure 2: Financial Fraud in the Digital Economy

As financial institutions transact millions of transactions on a day-to-day basis, it has become more difficult to detect fraud. It is not easy to monitor the data of such transactions manually. Besides, current fraudsters employ sophisticated approaches like synthetic identities, automated bots, and organized fraud networks that bypass fraud prevention systems [6]. AI and ML technologies are being widely used to solve these problems. By utilizing ML models, financial institutions can process vast amounts of transactions and gain insights into patterns and trends that may have gone unnoticed before, detect fraud patterns, and set up real-time fraud detection systems that can react quickly to suspicious transactions. With the help of ML models, financial institutions can analyze large datasets of transactions, uncover hidden patterns and trends, identify anomalies, and establish real-time fraud detection systems that can respond swiftly to suspicious transactions [7].

1.2 Role of ML and DL in Fraud Detection

The current fraud detection system has become a crucial part of the system using ML. In contrast to the old rule-based approaches, ML algorithms have the ability to use past data and adjust to the novel fraud patterns automatically [8]. In response to the past transactional pattern, various supervised learning models are commonly used to classify the transactions as fraudulent and legitimate: logistic regression, decision trees, SVM and the RF. DL methods have also helped in fraud detection, where high-dimensional and complex financial data has been analyzed, in the past few years. These subtleties in the transaction attribute relationship may not be captured by traditional ML methods, and DNN, CNN and RNN can see them [9].

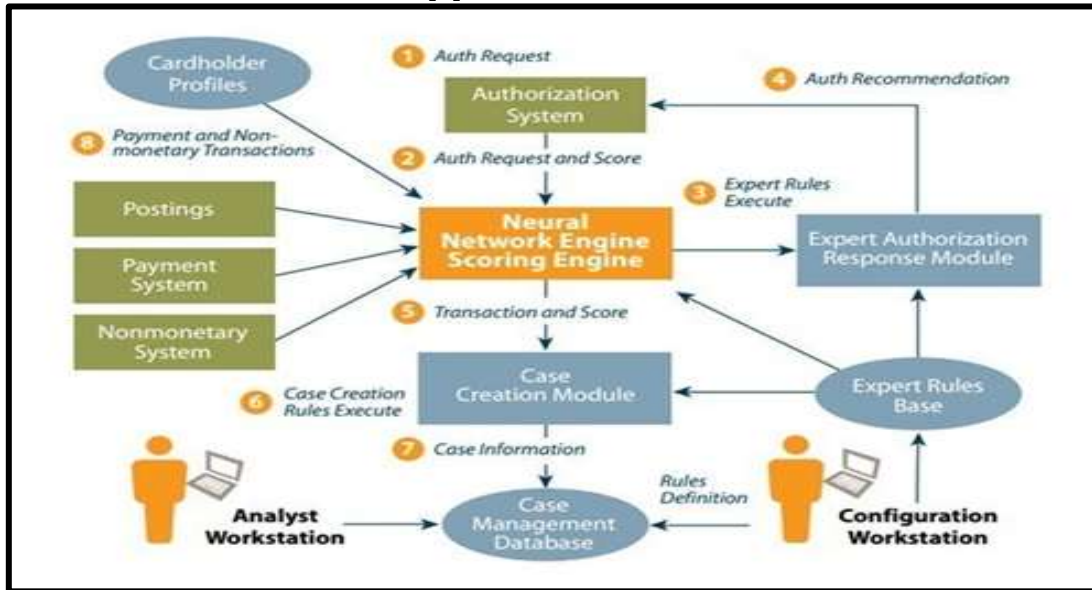


Figure 3: Role of ML and DL in Fraud Detection

Features can be extracted from hybrid models using statistical approaches and anomalies can be detected using statistical approaches. DL models can be used to carry out more complex pattern recognition and classification.

1.3 Hybrid ML Framework for Fraud Detection

The hybrid ML models are an innovative method of detecting financial fraud since they combine various methods of analysis into a single system. Statistical models, ML algorithms, and DL networks collaborate to process financial transactions information and detect fraudulent transactions in such structures in a more efficient way. The integration helps the system to identify not only easy statistical anomalies but also intricate patterns of behaviours related to fraudulent transactions [12]. The hybrid system is usually comprised of several steps, such as data preprocessing, feature extraction, anomaly detection, model training and fraud classification. Anomalous behavior in transaction data can be detected using statistical techniques like z-score analysis, probability distributions as well as correlation analysis [13].

Table 1: Hybrid ML Framework for Fraud Detection				
S.No.	Framework Component	Description	Techniques / Methods Used	Role in Fraud Detection
1	 Data Collection	Gathering large volumes of financial transaction data from banking systems, payment platforms, and financial databases.	Transaction Logs, Financial Databases, API Data Sources	Provides raw data required for training fraud detection models.
2	 Data Preprocessing	Cleaning and transforming raw transaction data to remove noise, missing values, and inconsistencies.	Data Cleaning, Normalization, Feature Scaling, Data Transformation	Improves data quality and prepares structured input for ML models.
3	 Feature Engineering	Extracting meaningful features from financial transaction data to represent behavioral patterns.	Statistical Feature Extraction, Correlation Analysis, Dimensionality Reduction	Helps identify relevant transaction characteristics associated with fraudulent activities.
4	 Statistical Analysis	Identifying anomalies and probabilistic irregularities in transaction data.	Z-score Analysis, Probability Distribution, Outlier Detection	Detects suspicious patterns based on statistical deviations.
5	 ML Layer	Applying supervised learning algorithms to classify transactions as legitimate or fraudulent.	Logistic Regression, RF, SVM, Decision Trees	Learns patterns from historical fraud data and predicts potential fraud.
6	 DL Layer	Analyzing complex patterns and hidden relationships within financial datasets.	Neural Networks, Deep Belief Networks, Autoencoders, LSTM Networks	Captures nonlinear relationships and evolving fraud patterns.
7	 Hybrid Model Integration	Combining statistical analysis, ML, and DL outputs to improve detection accuracy.	Ensemble Learning, Hybrid Modeling	Enhances fraud detection performance by leveraging multiple techniques.
8	 Fraud Classification	Final classification of transactions into legitimate or fraudulent categories.	Classification Algorithms, Probability Thresholding	Determines whether a transaction should be flagged as fraud.
9	 Model Evaluation	Using established measures to assess the efficacy of the fraud detection system.	Precision, Accuracy, F1-score, ROC-AUC, and Recall	Ensures reliability and effectiveness of the proposed framework.
10	 Real-Time Monitoring System	The ability to detect suspicious activity in real time through continuous surveillance of financial transactions.	Processing of Streaming Data in Real Time	Enables immediate fraud detection and prevention in financial systems.

Figure 4: Hybrid ML Framework for Fraud Detection

The neural network building capabilities of DL elements the hybrid framework can further develop transaction patterns with nonlinear relationships. The methods that are especially helpful in identifying previously unknown patterns of fraud are autoencoders, deep belief networks, and RNN. The hybrid models could be more precise in detecting the events and false positives are reduced due to combining the statistical knowledge with the potential of DL [14]. These days, hybrid fraud detection systems are in the spotlight because of the increasingly complex nature of fraudulent financial schemes. High-tech hybrid frameworks will allow financial institutions to have intelligent resources that will help them monitor financial transactions and detect suspicious activities as they occur and help in reducing financial losses that occur due to fraudulent activities [15]. So, in order to boost the effectiveness of fraud detection in finances, the designed hybrid ML model will be fused using statistical analysis and DL methodologies.

2. LITERATURE REVIEW

The latter investigations have been conducted on the hybrid ML techniques proposed so far, aiming at improving fraud detection accuracy. A hybrid ML model was suggested by Mohammed (2026) to combine various algorithms of classification to identify financial fraud more efficiently. The use of both traditional machine learning models and advanced learning techniques is shown to improve the predictive value and false positivity of financial transactions datasets. The results proved that ensemble learning techniques are significant in the processing of complex patterns of financial fraud and the large quantity of transactions data. [1]. The HybridFL framework proposed by Khan et al. (2026) is a federated learning-based model that can be used in financial crime

detection. In their study, they tackled privacy-sensitive ML in which many financial institutions train toxic fraud detection models jointly without the need to share sensitive information. The proposed solution has been found to be more successful in terms of detection of frauds and meanwhile has also given data confidentiality which is very crucial in the finance sector. The article highlighted the need to use decentralized methods of learning to have secure fraud detection systems. [2]. El Alami et al. (2026) examined quantum ML architecture application in detecting credit card fraud. The authors have compared the performance of several quantum based methods with the traditional ML methods and demonstrated that the computation performance and detection rate can be improved by using quantum enhanced methods. According to their work, quantum computing has started to become significant in a search for complex financial fraud cases. [3]. Kungu et al. (2026) suggested a hybrid DL model of detecting anti-money laundering with the unsupervised learning method. A model was used here to identify fraud patterns, leveraging feature fusion and explainable AI.

They discovered that uncontrolled DL models were able to identify the hidden financial crimes schemes that could not be easily discovered by traditional supervised systems, with a high accuracy. [4]. Dohare (2025) came up with a hybrid ML model that will be used to identify corporate management systems with financial fraud. The system consisted of a mix of the ML algorithms and statistical models which were applied to review the financial documents and detect the oddities. The results indicated that, in organizations, hybrid approaches positively affect the accuracy of financial information fraud detection to a great extent. [5]. The credit card fraud detection and anomaly detection in transaction terms were newly introduced by Alsagri (2025) by developing a multi-phase hybrid ML model. It was necessary to use multiple layers of classification in order to identify the fraud acts at multiple stages of the financial transactions. In the experiments results it was demonstrated that the multi-stage architecture increases the effectiveness of fraud detection and reduces the number of false alarms in the credit card transaction data. [6]. Boltaev and Rakhmatullaev (2025) have provided an extensive review of methods of AI in detecting fraud in financial sector. They reported on their research which evaluated different ML, DL as well as hybrid models used in fraud detection systems. The experiment showed that hybrid ML methods are more functional since it combines the advantage of statistical analysis and deep neural networks. [7]. Btoush et al. (2025) suggested a hybrid ML model of credit card fraud which consisted of stacking. Their model was an integration of several base classifiers by means of ensemble learning methods in order to increase predictive performance. [8]. Their study established that the combination of ML and risk-based financial measurements enhances performance of fraud detection in lopsided financial data. [11]. In a study titled "The Impact of AI on Financial Sector Cybersecurity Management," Mishra (2023) has examined the influence of AI-driven cybersecurity techniques on financial sector management. The authors have highlighted the importance of smart security systems for protecting financial infrastructures against cyber attacks and frauds in the study. [17]. The systematic literature review by Ali et al. (2022) focused on ML methods of financial fraud detection. They also compared the performance of different ML models and showed that the ensemble and hybrid ML models have superior detection performance compared to the single models. [18]. According to the study by Zhu et al. (2021), the financial fraud detection practice in the post-pandemic era has been researched. Their research highlights the importance of AI-driven solutions in the fight against fraud in the rapidly evolving digital financial landscape. [24]. Ashtiani and Raahemi (2021) have reviewed the literature thoroughly to understand and identify the ML techniques used to detect financial statement fraud. According to their research, the quality of the

financial reporting systems' fraud detection largely depends on high-quality ML models. [25].

3. PROBLEM STATEMENT

Monetary transactions have become more frequent and sophisticated as a result of the wide-spread use of ecommerce platforms, digital wallets, online banking, mobile payments and other digital financial solutions. These have made it easier to access, and easier to deceive! Some of the most pressing issues in today's banking world, and among regulatory agencies throughout the world, are credit card fraud, identity theft, money laundering, and fraudulent transactions [16]. These fraudulent behaviours can lead to damage of the reputation, a loss of consumers' trust in online financial services and significant financial losses. Traditional approaches to fraud detection heavily depend on the rule-based applications and most elementary statistical analysis techniques for detecting suspicious financial transactions. While these algorithms can pick up on preexisting fraud patterns, they aren't great at spotting the more complex patterns that fraudsters are using these days. Moreover, the conventional model has a difficulty in determining fraud with a high accuracy, since the amount of fraudulent transactions is a very small proportion of all transactions and financial transaction data is highly skewed [17]. Patterns of complex behavior can be identified through the analysis of large financial data sets, and this is where ML and DL approaches have proven to be useful. But, with large, heterogeneous datasets and constantly evolving fraud patterns, specific models can be ineffective. This underlines the importance of an advanced hybrid framework to combine ML and DL with statistical analytic techniques. Such a hybrid ML approach can be used to identify financial fraud in the existing financial system, detect abnormalities, and boost the effectiveness of fraud detection [18].

4 RESEARCH METHODOLOGY

The proposed research methodology involves creating a Hybrid Machine Learning Framework for Financial Fraud Detection, which combines statistical analysis, Machine Learning (ML), and Deep Learning (DL) methods. The methodology starts by extracting data related to financial transactions including fraudulent and legitimate transactions [19]. To enhance the quality of the dataset, data preprocessing techniques like data cleaning, normalization, dealing with missing values, and SMOTE balancing are used to handle imbalanced datasets. Once the data has been pre-processed, feature engineering techniques are used to identify and create relevant features that capture information about the transactions, including the amount of the transaction, the time and place of the transaction, and the patterns of user behavior. Then anomalous transactions are detected using statistical anomaly detection techniques such as Z-score analysis [20]. Classifiers such as Logistic Regression, SVM and Random Forest are implemented using traditional ML techniques and are used for fraud classification. Furthermore, the use of DL models like ANN and LSTM networks is employed to learn complex and non-linear fraud patterns. A hybrid ensemble approach is adopted to combine the outputs of the statistical analysis and the ML models and DL networks, to enhance the fraud detection accuracy and reduce the number of false positives [21]. Lastly, the framework is tested with various performance measures like Accuracy, Precision, Recall, F1-Score and ROC-AUC. The implementation is done in Python, TensorFlow, Keras, Scikit-learn, and Jupyter Notebook environment [22].

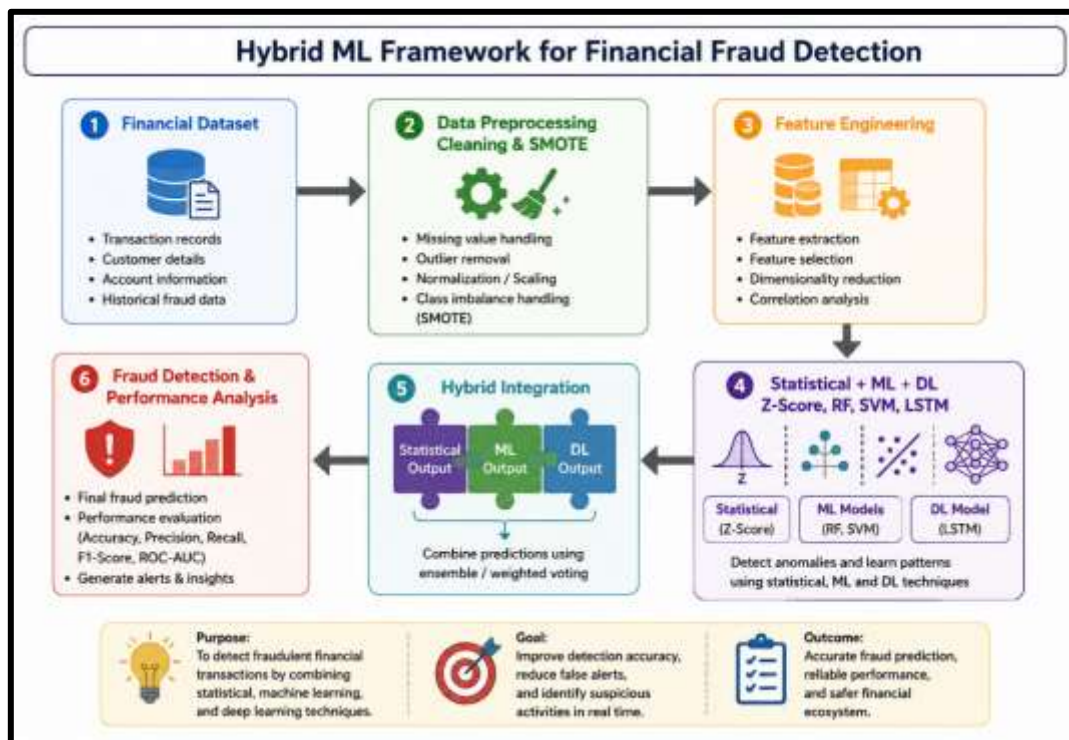


Figure 4: Research Methodology

The Hybrid Machine Learning Framework for Financial Fraud Detection is a comprehensive and intelligent system designed to identify fraudulent financial transactions by integrating statistical analysis, machine learning, and deep learning techniques into a unified framework. The process begins with the collection of financial transaction datasets from multiple sources such as banking systems, online payment gateways, digital wallets, and financial databases. These datasets contain transaction records, customer information, account details, transaction amounts, timestamps, geographical locations, and historical fraud labels. Since raw financial data often contains missing values, inconsistencies, duplicate records, and noise, the framework first performs data preprocessing to improve data quality and reliability. Techniques such as data cleaning, normalization, scaling, outlier removal, and Synthetic Minority Oversampling Technique (SMOTE) are applied to balance the dataset and reduce the impact of class imbalance, where fraudulent transactions are significantly fewer than legitimate transactions. This preprocessing stage ensures that the input data becomes structured, consistent, and suitable for advanced analytical modeling. After preprocessing, the framework performs feature engineering to extract meaningful and informative characteristics from the transaction data. This stage identifies behavioral and transactional patterns associated with fraudulent activities. Feature extraction methods, dimensionality reduction, correlation analysis, and statistical feature selection techniques are used to reduce redundancy and improve the predictive capability of the dataset. The extracted features are then passed through a statistical analysis layer where anomaly detection methods such as Z-score analysis, probability distribution analysis, and outlier detection are employed to identify suspicious transaction patterns that significantly deviate from normal behavior. These statistical approaches provide an initial indication of potentially fraudulent transactions and help improve the sensitivity of the overall fraud detection system. The framework further integrates machine learning and deep learning layers to enhance fraud prediction accuracy. In the machine

learning layer, supervised learning algorithms such as Logistic Regression, Random Forest, Support Vector Machine (SVM), and Decision Trees are trained using historical transaction data to classify transactions into legitimate or fraudulent categories. These algorithms learn transaction patterns and decision boundaries from labelled datasets to predict fraudulent behavior effectively. Simultaneously, the deep learning layer uses advanced neural network architectures such as Artificial Neural Networks (ANN), Autoencoders, Deep Belief Networks (DBN), and Long Short-Term Memory (LSTM) networks to capture complex nonlinear relationships and hidden temporal patterns within financial transactions.

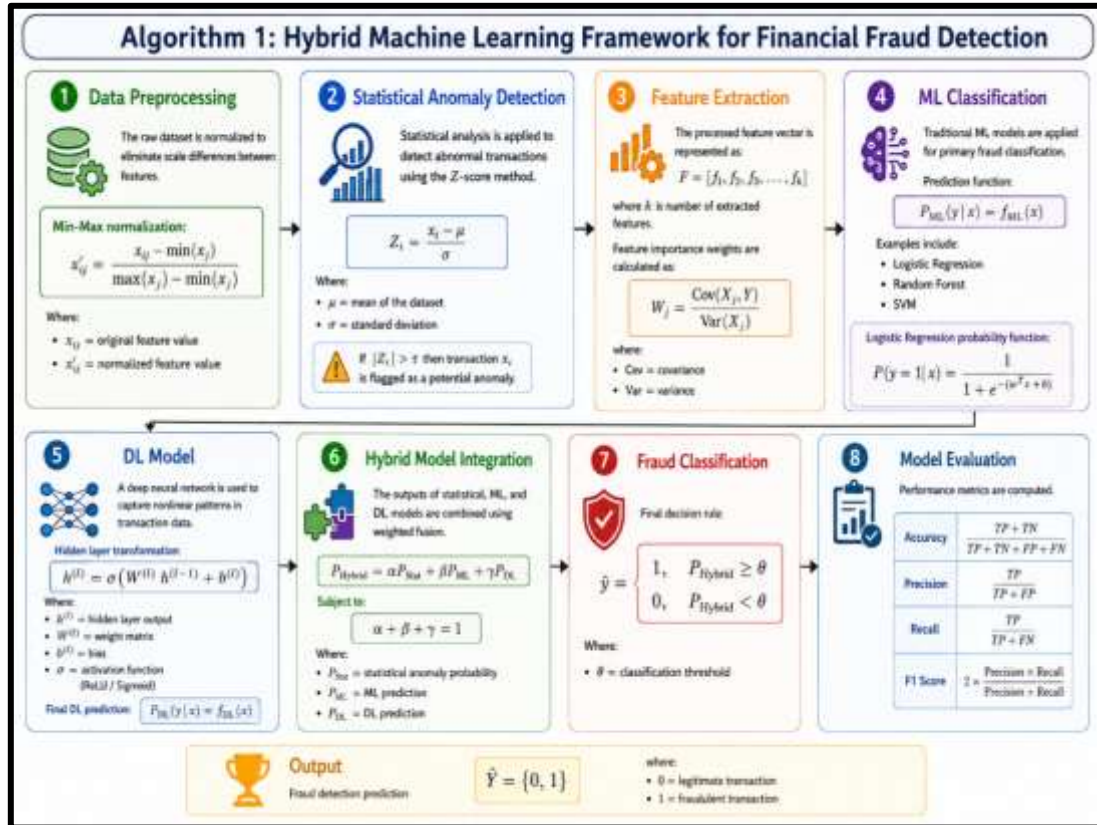


Figure 5: Hybrid Machine Learning Framework for Financial Fraud Detection

5. NOVELTY OF THE WORK

The proposed research project, “Hybrid ML Framework for Financial Fraud Detection Using Statistical and Deep Learning Models”, proposes a new and innovative approach to a financial fraud detection problem that uses a combination of a statistical model and a deep learning model to boost the accuracy of fraud identification in the modern financial system [23]. The proposed hybrid model combines statistical anomaly detection, feature optimization, and deep neural network architectures to enable powerful, adaptive, and real-time fraud detection [24]. The novelty of this work is the following aspects:

- **Hybrid Detection Architecture:** The framework is based on a combination of statistical analysis methods and Deep Learning models like ANN, LSTM or Autoencoders to identify known and unknown fraudulent transaction patterns [25].

- **Multi-Level Fraud Analysis:** The proposed model performs fraud detection at the behavioral, transactional and temporal levels, which can detect the sophistication fraud activities that traditional methods may not be able to detect.
- **Dynamic Feature Learning:** The DL component automatically learns hidden transaction patterns and adapts to changes in fraud patterns over time, while reducing the need for manual effort [26].
- **Increased accuracy and lower false positives:** The framework combines the statistical filtering with DL classification to minimize the number of FAs and enhance the precision, recall, and F1 score of the detection [27].
- **Scalable Real-Time Detection:** The proposed framework is suitable for large-scale digital banking and online payment contexts where real-time fraud monitoring is crucial [28].
- **Improved Financial Security Scope:** The work offers a future-proof fraud detection solution that can be applied to banking systems, e-commerce platforms, digital wallets, and fintech applications.

6. RESULTS AND DISCUSSIONS

In this part, we provide the results of the experiments conducted using the proposed Hybrid ML Framework for Detecting Financial Fraud using Statistical and DL Models. The performance of the proposed model is evaluated using a number of DL approaches, hybrid models and ML algorithms. Its assessment was based on popular metrics for measuring the effectiveness of fraud detection systems: accuracy, precision, recall, F1-score and ROC-AUC. Any type of financial transaction, whether fraudulent or not, was tested. From the findings, it appears that the hybrid model proposed is better than the single models in the ability to detect fraud instances.

6.1 Experimental Setup

The experimental framework consists of model training, model performance evaluation, data preprocessing, and feature extraction. The first thing that had to be done was to eliminate inconsistencies and missing information from the bank records of the transactions. The data was statistically normalized using any of the data normalization methods before being entered into the ML models. Several ML models such as Logistic Regression, random forest, support vector machine models were used to compare baseline performance. Moreover, the ANN and LSTM networks have been applied to study complex transaction patterns of DL networks. Lastly, a model was designed based on statistical analysis, ML and DL for improving the efficiency of fraud detection. Details on the dataset utilized to train and test the suggested model, as well as the total number of transactions, the proportion of fraudulent to valid ones, and other pertinent information can be found in Table 3.

Table 2: Dataset Description

Parameter	Description
Dataset Type	Financial Transaction Dataset
Total Transactions	284,807
Fraudulent Transactions	492
Normal Transactions	284,315

Number of Features	30
Data Imbalance Ratio	Highly Imbalanced

The problem of fraud detection is a difficult classification problem as there is a highly skewed number of valid and fraudulent transactions in the dataset.

6.2 Performance Comparison of Individual Models

An assessment of each of the ML models was conducted independently to determine the model's capacity for fraud detection. The findings suggest that conventional models perform averagely and are not able to pick up complicated patterns of fraud.

Table 4 shows the performance (accuracy) of each of the ML models used for financial fraud detection. We used the measures presented below in the table to compare the algorithms with respect to their ability to detect fraudulent transactions.

Table 3: Performance of Individual ML Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score
Logistic Regression	94.2	89.3	82.5	0.85
Support Vector Machine	95.6	90.4	84.1	0.87
Random Forest	96.8	92.7	88.9	0.90

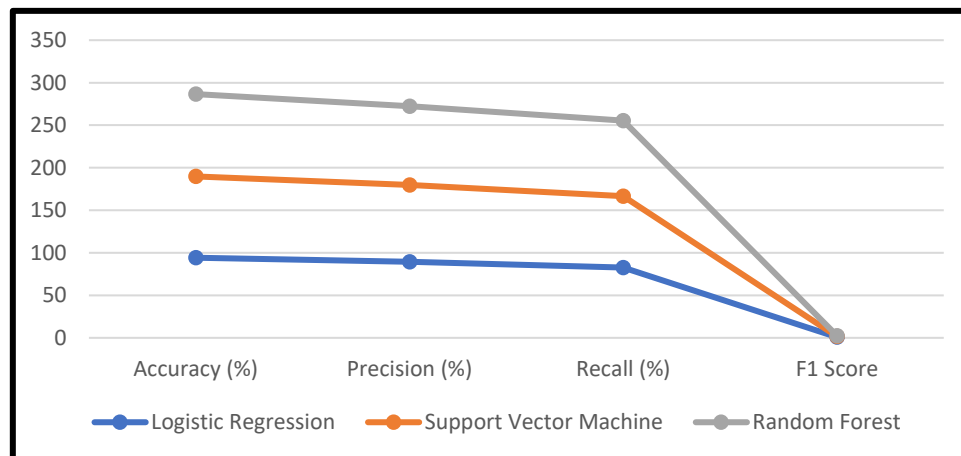


Figure 6: Performance of Individual ML Models

Figure 5 shows a comparison of the performance of various financial fraud detection ML models. As it can be seen from the figure, the various classification algorithms have showed a wide range of accuracy in identifying the fraudulent transactions with respect to KPIs. The largest benefit of using random forest over traditional models was its ability to deal with the nonlinear relationships and complex interactions between data.

6.3 Performance of Deep Learning Models

The capacity of DL models to uncover hidden patterns in the transaction data was evaluated through testing. The results of the performance analysis of the DL models used to detect financial fraud in this paper are displayed in Table 5. The table compares the

models' efficacy according to the major performance indicators; all of them are competent enough to detect complex patterns of fraud in data on financial transactions.

Table 4: Performance of DL Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score
Artificial Neural Network	97.2	93.5	90.4	0.91
LSTM Network	97.9	94.6	91.8	0.93

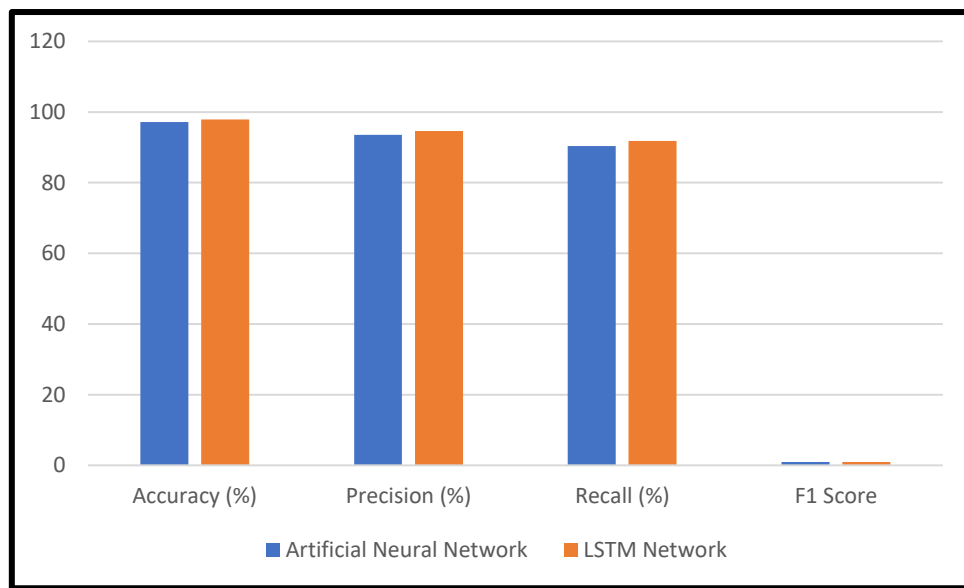


Figure 7: Performance of DL Models

The outcome of the study's performance analysis of the DL models is shown in figure 7. The chart illustrates the most important metrics to support DL techniques' ability to uncover complex patterns and enhance the accuracy of financial fraud detectors. The result demonstrates that DL models are able to learn complex nonlinear pattern with huge amount of data which is more advantageous than traditional ML models.

6.4 Performance of Proposed Hybrid Model

The proposed hybrid approach combines statistical anomaly detection, ML classification and DL pattern recognition techniques to improve the effectiveness of fraud detection. From the table, it is observed that hybrid (hybrid model using statistics, ML and DL) is more efficient with regard to important performance measures. This is an indication that the hybrid is more accurate and reliable.

Table 5: Performance of the Proposed Hybrid Model

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score	ROC-AUC
Proposed Hybrid Model	98.9	96.8	95.2	0.96	0.99

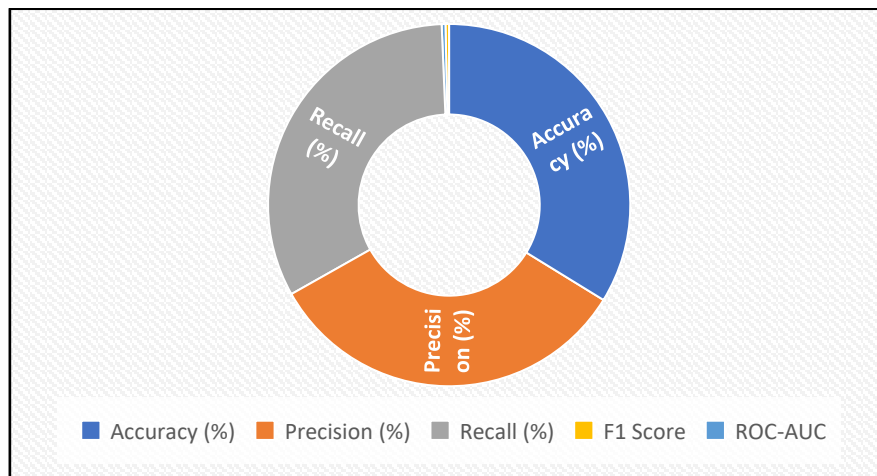


Figure 8: Performance of the Proposed Hybrid Model

The figure shows the assessment criteria used to assess the power and reliability of the hybrid approach in reducing misclassifications and increasing fraud detection accuracy. All the evaluation metrics showed the better performance of the hybrid model. Combining DL with statistical analysis improved the system's ability to perpetrate fraud while also decreasing the amount of false positives. As evidenced by the confusion matrix, the hybrid model achieved a good rate of accuracy in identifying most of the fraudulent transactions without any significant false positives. The results of the experiments indicate that the hybrid models outperform the conventional ML and DL models used individually in terms of fraud detection. Classification algorithms are very useful for machine learning and statistical processing can be used to detect suspicious transactions. A DL model's ability to shed light on the intricate patterns of behavior in financial transaction data is an extra step toward system improvement. This combination of methodologies leads to a hybrid framework with better accuracy, recall and reduction in false positive rate. The hybrid model has the other benefit of being able to uncover unique fraud patterns that the rule-based or mono model techniques would not be able to detect. The hybrid ML system proposed in general is a viable alternative to traditional methodologies for financial fraud detection. Financial institutions may now accurately detect fraud situations and respond to any security concern quickly. The experimental results reveal that the proposed framework is promising to improve significantly the robustness and efficiency of fraud detection systems in real-world financial contexts.

7. CONCLUSION

The nature of fraudulent schemes is changing and the volume of financial transactions is expanding dramatically, making financial fraud harder to detect. Statistical models and rule-based solutions fail to detect complicated fraud tendencies. The purpose of this work is to construct a hybrid ML framework that combines deep learning models with statistical learning methods to improve the performance of fraud detection. The suggested method benefits from the deep neural network and statistical inference to produce an effective and flexible system for fraud detection. Future work will be dedicated to the integration of novel DL structures such as explainable AI techniques as well as transformer models to enhance the model performance and transparency.

8. FUTURE SCOPE

The existing basic hybrid ML can be improved with more sophisticated AI techniques and a wider real-world financial dataset for detecting financial fraud. Areas for future study include building fraud detection systems that leverage streaming data analytics to monitor monetary transactions as they occur in real time. Another way to improve the framework is to model the interactions between users and transactions using more advanced DL structures, e.g., the transformer model and graph neural networks. XAI methods can be employed to increase the transparency and interpretability of fraud detection systems in financial organizations. Two other potential future uses are federated learning, which prevents the sharing of sensitive financial data between institutions to detect fraud, and generative AI. Two more future prospective applications are federated learning and generative AI which could aid with fraud detection without moving data between institutions. Generative AI could likewise be used to create synthetic data and images for the same purpose. Security and fraud protection are important for digital financial ecosystems and the hybrid ecosystem can play a part here. Hybrid approach can help to increase the security and anti-fraud measures, which are the basis of the validity of digital financial system.

REFERENCES

1. Mohammed, R. (2026). Enhancing Fraud Detection with Hybrid ML Models. *International Journal of Applied Data Science & Modern Computing*, 1(1), 14-26.
2. Khan, A., Thij, M. T., Tang, G., & Wilbik, A. (2026). HybridFL: A Federated Learning Approach for Financial Crime Detection. *arXiv preprint arXiv:2602.19207*.
3. El Alami, M., Innan, N., Shafique, M., & Bennai, M. (2026). Comparative performance analysis of quantum ML architectures for credit card fraud detection. *Applied Intelligence*, 56(3), 83.
4. Kungu, C. O., Senagi, K., & Omondi, E. (2026). Hybrid DL for anti-money laundering: Unsupervised detection of emerging schemes via feature fusion and explainable AI. *ML with Applications*, 23, 100856.
5. Dohare, A. K. (2025). A Hybrid ML Framework for Financial Fraud Detection in Corporate Management Systems. *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, 46(02), 139-154.
6. Alsagri, H. S. (2025). Hybrid ML based multi-stage framework for detection of credit card anomalies and fraud. *Ieee Access*.
7. Boltaev, F. H., & Rakhmatullaev, N. G. (2025). AI TECHNIQUES FOR FINANCIAL FRAUD DETECTION: A COMPREHENSIVE REVIEW OF ML, DL, AND HYBRID MODELS. *Economics and Innovative Technologies*, 13(2), 160-174.
8. Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., & Alsodi, O. (2025). Enhancing credit card fraud detection with a stacking-based hybrid ML approach. *PeerJ Computer Science*, 11, e3007.
9. Yu, G., & Luo, Z. (2025). Financial fraud detection using a hybrid deep belief network and quantum optimization approach. *Discover Applied Sciences*, 7(5), 454.
10. Mark Lokanan, Satish Sharama, "The use of ML algorithms to predict financial statement fraud", Published by Elsevier Ltd., 14 July 2024.
11. ABDULLAHI UBALE USMAN, SUNUSI BALA ABDULLAHI, YU LIPING, BAYAN ALGHOFAILY, AHMED S. ALMASOUD AND AMJAD REHMAN, "Financial Fraud Detection Using Value-at-Risk With ML in Skewed Data", Digital Object Identifier 10.1109/ACCESS.2024.3393154, 24 April 2024

12. YUXUAN TANG AND ZHANJUN LIU, "A Distributed Knowledge Distillation Framework for Financial Fraud Detection Based on Transformer", Digital Object Identifier 10.1109/ACCESS.2024.3387841, 11 April 2024
13. Surendranadha Reddy Byrapu Reddy, Praneeth Kanagala, Prabu Ravichandran, Dr Rahul Pulimamidi, P.V. Sivarambabu, Naga Simhadri Apparao Polireddi, "Effective fraud detection in e-commerce: Leveraging ML and big data analytics", Published by Elsevier Ltd., 10 April 2024
14. Paulin K. Kamuangu, "A Review on Financial Fraud Detection using AI and ML", Journal of Economics, Finance and Accounting Studies, ISSN: 2709-0809, DOI: 10.32996/jefas, Journal Homepage: www.al-kindipublisher.com/index.php/jefas, 11 February 2024
15. Debidutta Pattnaik, Sougata Ray, Raghu Raman, "Applications of AI and ML in the financial services industry: A bibliometric review", Published by Elsevier Ltd., 13 December 2023
16. ZIWEI YI, XINWEI CAO, ZUYAN CHEN AND SHUAI LI, "AI in Accounting and Finance: Challenges and Opportunities", Digital Object Identifier 10.1109/ACCESS.2023.3333389, 16 November 2023
17. Shailendra Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management", Appl. Sci. 2023, 13, 5875. <https://doi.org/10.3390/app13105875>
18. Abdulalem Ali, Shukor Abd Razak, Siti Hajar Othman, Taiseer Abdalla Elfadil Eisa, Arafat Al-Dhaqm, Maged Nasser, Tusneem Elhassan, Hashim Elshafie and Abdu Saif, "Financial Fraud Detection Based on ML: A Systematic Literature Review", Appl. Sci. 2022, 12, 9637. <https://doi.org/10.3390/app12199637>
19. Ajeet Singh, Anurag Jain and Seblewongel Esseynew Biabile, "Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine", Hindawi, Applied Computational Intelligence and Soft Computing, Volume 2022, Article ID 1468015, 10 pages, 17 June 2022
20. Ieva VOSYLĪŪTĒ, Nijolė MAKNIČIENĒ, "Investigation of Financial Fraud Detection by Using Computational Intelligence", Published by Vilnius Gediminas Technical University, May 12–13, 2022
21. JiaoLong Li, "E-Commerce Fraud Detection Model by Computer AI Data Mining", Hindawi, Computational Intelligence and Neuroscience, Volume 2022, Article ID 8783783, 9 pages, 9 May 2022
22. FAWAZ KHALED ALARFAJ, IQRA MALIK, HIKMAT ULLAH KHAN, NAIF ALMUSALLAM, MUHAMMAD RAMZAN AND MUZAMIL AHMED, "Credit Card Fraud Detection Using State-of-the-Art ML and DL Algorithms", Digital Object Identifier 10.1109/ACCESS.2022.3166891, 12 April 2022
23. Waleed Hilal, S. Andrew Gadsden, John Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances", Published by Elsevier Ltd., 31 December 2021
24. Xiaoqian Zhu, Xiang Ao, Zidi Qin, Yanpeng Chang, Yang Liu, Qing He and Jianping Li, "Intelligent financial fraud detection practices in post-pandemic era", October 20, 2021
25. MATIN N. ASHTIANI AND BIJAN RAAHEMI, "Intelligent Fraud Detection in Financial Statements Using ML and Data Mining: A Systematic Literature Review", Digital Object Identifier 10.1109/ACCESS.2021.3096799, 13 July 2021
26. DATTATRAY VISHNU KUTE, BISWAJEET PRADHAN, NAGESH SHUKLA AND ABDULLAH ALAMRI, "DL and Explainable AI Techniques Applied for Detecting Money Laundering: A Critical Review", Digital Object Identifier 10.1109/ACCESS.2021.3086230, 4 June 2021

27. Kalusivalingam, A. K., Sharma, A., Patel, N., & Singh, V. (2020). Enhancing financial fraud detection with hybrid DL and random forest algorithms. *International Journal of AI and ML*, 1(3).
28. Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A financial fraud detection model based on LSTM DL technique. *Journal of Applied Security Research*, 15(4), 498-516.