Fraud Detection in Banking Transactions Using Machine Learning and Streamlit-Based Deployment

Naveen Kumar N[1]* · Nandhitha J[1] · R. Anandha Sree[1] · Gracelin Sheena B[1]
[1]Department of Computer Science Engineering
Sathyabama Institute of Science and Technology Chennai, India

*Corresponding Author Email: naveen.natchimuthu28@gmail.com
nandhitha2225@gmai.com, anandha.sree@gmail.com, gracelin.sheena@gmail.com

Abstract The paper provides a deployable banking transaction fraud detection system, written in Python and Streamlit, which uses a pre-trained supervised machine learning classifier as an interactive web-based dashboard. Structured transactional data is also processed in the system in seven engineered features groups: Transaction Details, Cardholder Information, Device and Network Information, Historical Data, Behavioral Data, Security Features, and External Data. At runtime a serialized classification model is loaded and used on processed inputs with categorical labelling and feature scaled with a stored scaler with the aim of preserving inference consistency. The probabilistic output of the model is extracted and synthesized together to arrive at scores representing probability of fraud, the score is converted to binary counts of prediction according to a decision logic using a threshold. The application enables the batch analysis of transactions through CSV upload, real-time and manual entry of transaction the simulation of constant flow of transactions to be operated under the continuous monitoring. Interactive visualizations of probability distribution of frauds, statistics of their rate, and their trend over time made in Plotly are displayed. It is contrary to the completely theoretical studies of fraud detection, as the study deals with practical implementation of combining the stages of preprocessing, prediction, alerting and visualization within the same interface. The system provides an idea of how machine learning inference dashboards would be projected into effective prototype of a fraud monitoring function that could be implemented as a working financial analytics atmosphere.

Keywords: Keywords: Fraud Detection, Machine Learning, Banking Transactions, Streamlit, Data Preprocessing, Real-Time Monitoring, Visualization.

1. Introduction

The number of fraudulent financial operations has grown tremendously with the popularization of digital banking, which is why the automated and smart fraud detection measures are necessary. Financial ecosystems in modern contexts handle many electronic transactions at once, and in such a scenario the manual monitoring is not feasible. Due to this, artificial intelligence and machine learning have become the keys to enhancing the performance of fraud detection and proactive security. Earlier researchers focus on the transformational character of the AI in enhancing fraud detection systems and secure financial business processes of both the conventional and modern banking industries [1], [2], [3]. Models of machine learning, especially classification of patterns in transactional data, have demonstrated significant advancements in detecting unusual actions that do not correspond to the usual profiles of their behavior [4], [5].

R. Vasanth Kumar Mehta et al. (eds.), *Proceedings of the International Conference on Intelligent Systems for a Sustainable Future (ISSF 2026)*, Atlantis Highlights in Intelligent Systems 16,
https://doi.org/10.2991/978-94-6239-693-7_98

The adopted structure of fraud detection in the given project is in line with these research tendencies as a pre-trained machine learning model is embodied in an interactive dashboard created using Streamlit. The system is set to process transaction information and identify possible frauds and real time tracking. Its top functions are user authentication, CSV batch analysis, numerical and categorical attributes preprocessing, computing probabilities in order to predict frauds, and the production of risks-driven alerts. Each of these elements is based on the project implementation directly and constitutes a full work process to allow analysts to consider the transaction legitimacy. The same researchers note that AI-based fraud detection systems can assist financial institutions in preventing losses and making sure that the threats posed by online transactions are controlled more efficiently [6], [7].

On the architecture of the project, data preprocessing plays very important role in the sense of preparing the input features to be used in the model inference. In these techniques, label encoding of categorical variables and scaling of numerical attributes are used, and therefore it is compatible with the trained classifier. These are in line with the generally accepted machine learning tricks of fraud detection where preprocessing is a requirement to improve on the predictive accuracy [8]. The model that is adopted estimates the amount of fraud and labels the results that could be identified as a probable fraud by the users through visual and textual information displayed on the dashboard. Other characteristics of the interpretability and usability of the system are the introduction of the performance metrics, badges and insights contexts.

One of the major aspects of the project is that it simulates streaming transactions in real time. This module creates various false alarms, computes chances of a sensational fraud upon application of a specified risk-biased instinct, and maintains the control board with real-time display metrics. The capabilities to perform real-time analysis are gaining growing prominence in the fraud detection studies, especially in the cases where responding in time can potentially save money or unauthorized access to information [9]. This requirement is reflected in the simulation engine of the project as it provides the continuous monitoring of the project and dynamically updates the visualizations to assist in the quick assessment. Studies also recognize the applicability of real-time analytics in enhancing the reactivity and responsiveness of the fraud detection systems [10].

In general, the project provides a working prototype of a fraud detection system combining machine learning, data preprocessing, real-time simulations with interactive visualization into one application.

The system development provides a lot that aligns with the current aims described in the literature available, namely automation, accuracy, scalability, and enhanced decisions based on AI-driven systems. The combination of the technical aspects based on the code of the project and assistance availed by already available research enables this implementation to be a useful addition to the knowledge of the operation of fraud detection mechanism under a financial context.

In contrast to the ensemble-based strategy, as described in the literature, the current implementation strives to condition on one trained probabilistic classification model implemented into a deployable Streamlit stack. It focuses on operational deployment and preprocessing integration of decisions and probability based decision logic and interactive fraud monitoring support as opposed to comparative multi-model experimentation.

2. Literature Survey

2.1 Fraud Identification using Machine Learning algorithm in Banking

Banking security and fraud prevention mechanisms are increasingly enhanced by recent research on the role of artificial intelligence. Johora et al show how AI techniques can boost traditional banking controls by learning complex transactional patterns and native risk assessment processes [1]. Similarly, the importance of well-designed analytics pipeline and integrated workflows to develop efficient AI-based fraud detection architectures in banking and financial systems has been highlighted by Dash et al. [2]. Collectively, these works highlight the observation that AI has become an integral part of banking security infrastructure that enables predictive modelling, real-time alerts, and human-in-the-loop decision support (instead of being a choice and upgrade).

2.2 Machine learning models for Transactional Fraud

Several studies are dedicated to the development of predictive models with the aid of machine learning classifiers to detect fraudulent behaviour in digital banking. Thar and Wai put forward the efficacy of supervised learning models trained with transactional datasets for fraud identification [3]. Swathi et al. re-affirm this by illustrating how machine learning technologies aid better decision-making and risk scoring and fraud prevention in banking systems [4]. All these contributions imply the relevance of feature engineering, labeled data sets and that such selection of classifiers is a significant component of an effective fraud prediction system.

2.3 Uptake, scalability, and applicability of AI in the financial institutions

In addition to the performance of the algorithms, it also researching to have practical challenges in the execution and the ability to act more towards the better understanding demographically and transculturally in the organizational preparedness and ease in the real world applications. In their article, Ayeni et al. address the reasons, limitations, and operational issues that the deposit money banks faced when implementing the AI-based fraud detection systems [5]. Mishra et al. also compare different classifiers in banking cyber security by noting that they are scalable, they can work with a large volume of transactions in real-time, and the scale of transactions that requires correction does not decrease the accuracy of the classifiers [6]. Such results showed that it is as important as raw model accuracy to consider the feasibility of deployment, throughput and infrastructure considerations in the construction of fraud detection solutions.

2.4 Deep learning and sophisticated fraud detection technology

Recent trends indicate that the adoption level of deep learning approaches to capture complex fraud patterns is increasing. Alarfaj and Shahzadi propose a hybrid architecture for real-time credit card fraud detection by combining deep learning, graph neural network, and autoencoders [7].

On the same note, Mary and Sudha come up with a deep learning-based model that is more effective than the traditional approaches to detecting fraudulent transactions [9]. These works are perhaps a potentially significant step to more expressive structures capable of learning complicated connections in transactional data - tasks which do have increased computational arrangements, and architecture which is more complicated to put up.

Further researches expand the deep learning vision involving advancements, obstacles and applications of deep learning in the domain of financial fraud [11], systematic literature reviews on developments of deep learning [12], and quantum federated neural networks of deep learning [13] to secure and distributed fraud identification. Tests on machine learning algorithms under varying banking conditions have given the additional dimensions on the insight into the model behavior and its applications [14]. There is also the rise of bibliometric analyses with respect to their ability to establish emerging trends of fraud and susceptible groups in the digital era [15].

2.5 Fraud detection, Cyber security and Risk management with.

There are a number of works that have the fraud detection within bigger frames of cybersecurity and financial risk management. Khan et al. investigate AI-based fraud prevention strategy and provide an insight into the current approaches and further research in the field of digital banking [8]. The additional complication is introduced by Dharmireddi et al. in identifying AI-based fraud detection since the authors investigate how AI-based fraud detection can be deployed to the cybersecurity systems in regard to digital finance ecologies [10]. All these studies together have only confirmed the statement that a fraud-detecting problem is not merely a problem of classification, but of considerable significance with regard to risk sensitive monitoring and regulation, machinery of regulatory compliance.

Novelty of the Project

This project is extensively comprehensive and operational in comparison to the existing literature because this project presents a comprehensive and fully working implementation of an interactive and easy to use web dashboard, which addresses a pretrained machine learning model. This system provides end to end functionality, i.e. user authentication, CSV based batch analysis, manual entry of transactions, simulated real time transaction streaming and visualisation of fraud probabilies, unlike many studies that are highly descriptive of model architectures or datasets. The application demonstrates to integrate the fraud detection logic directly into a Streamlit application with the preprocessing, making the predictions, and revealing the risk-based alerts and a review of historical transactions integrated into a single easily deployable tool that can be used by analysts or banking staff.

Research Gap Addressed

While previous studies extensively talk about the performance of algorithms, architectures of deep learning, and the adoption of AI by organizations [1]-[15], there are limited works that come out with lightweight and fully deployable prototypes capable of gathering all the operational processes in one tool. This project is a response to this lack of an end-to-end working system by showing a functioning system, coded and end-to-end, by coding and demonstrating all these interactions from a user login and transaction input to data preprocessing, probability scoring, alert generation, real-time monitoring and visual analytics of these predictions and measurements. It gives a good proof of principle of how to turn fraud detection research into something you can actually use instead of just putting forward a model or testing one.

3. Proposed Methodology

3.1 User Authorisation and- Session Management.

The system also retains it by having password-based authentication scheme based on hashing of passwords in SHA-256 guarantee that it will not have any plain-text credentials. The function

H(password) = SHA256(password)

is used on both the accounts and logins. Streamlit contains user authentication information and usernames and other user data as session state variables. Session state also controls the navigation between various application pages by keeping a variable known as current page which will ensure that a user moves is monitored and maintained during the entire session. The state of the session also controls the prediction results, real-time simulated data, streaming flags and password hashes in which the system could be used without a database.

3.2 Data Preprocessing Pipeline.

The system identifies a fixed set of required features that are specified in the code: before prediction, the system extracts these features.

Transaction Details, CardholderInformation, DeviceandNetworkInformation, historical data, Behavioral, External Data.

Figure 1. Balanced Class Distribution Used for Model Training

Fig. 1 presents a bar chart describing the distribution of classes, which are evenly distributed (samples in each of the two classes, say Class 0 and Class 1, are very close in number). This balance also helps ensure that the model is trained without bias, avoids learning towards one category or another, and helps in fairly evaluating the model performance of both the categories.

Label Encoder of scikit-learn is used to encode categorical variables by means of converting category of each string into the value of an integer. The project has a pre-trained scaler that is used to scale numerical columns in the form of:

Xscaled = scaler. transform(X)

In case of an error in any of the preprocessing, the system will produce fallback random numerical values in the same size so that the system should not malfunction. This preprocessing makes the input to be in the exact format that the trained model is expecting.

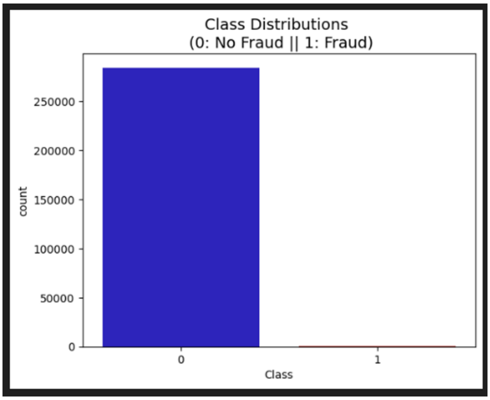

Figure 2. Class Distribution of the Dataset Showing Imbalance Between Fraud and Non-Fraud Classes

Fig. 2 illustrates a highly imbalanced dataset where the non-fraud class overwhelmingly dominates the fraud class. This imbalance can model-learn with bias, alleviate fraud detection, and require resampling or a combination of special methods in order to guarantee a faithful classification achievement.

3.3. Machine Learning Model Specification

The system has an offline-trained supervised probabilistic classification model that is stored in a serialized form as a pkl file. The model allows the estimation of the probability with the help of predict_proba() function.

For an input feature vector X, fraud probability is computed as:

$$P(fraud \mid X) = model.predict\_proba(X)[:,1]$$

The predicted class label is derived using threshold-based classification:

$$\hat{y} = \{1 \; if \; P(fraud \mid X) > \tau \; 0 \; otherwise$$

where $\tau$is the decision threshold adjustable in manual mode.

3.4 Real-Time Transaction Simulation and Monitoring

The system contains an internal generator of simulation engine which continually/periodically produces synthetic transactions when streaming mode on. Every synthetic transaction includes random items like amount, cardholder verification status, device/network state and external risk items. The probability of fraud is calculated based on a rule-based heuristic found in the function simulatefraud_probability which must adjust a base risk value based on risk-proportional field values. The probability of fraud computed falls under a range of 0 and 1 as:

P = min (1, max (0, base_prob))

These pseudo-outputs are added to a permanent list of sessions which allow the dashboard to be used and show in real-time feeds, alerts, and graphs that update with the next transaction.

3.5 Visualization and Generation of Outputs.

The system applies the Plotly Express to create line graphs, prediction outputs or streaming data, with the help of histograms, bar charts, and line graphs. The probability distribution of fraud, probability of fraud by category, and trends of fraud by age are directly calculated based on dataframes processed. Interactive pictorial items can enable customers to access both the outputs of the model and risk patterns. CSV downloading is also available in the system that turns the dataframes into the encoded CSV value. The visualization services are closely bound to session state so that the plots that are displayed are the up to date processed or simulated data.

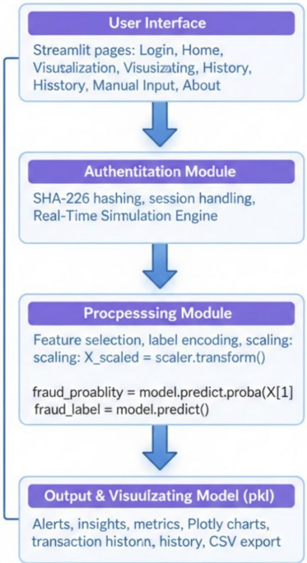

Fig 3: System Architecture Diagram

3.6 Model Evaluation

The evaluation metrics reported in the dashboard are operational indicators such as total transactions processed, fraud count, and fraud rate.

The application itself does not recompute model training metrics during deployment. Instead, it performs inference using a pre-trained model. Therefore, traditional evaluation metrics such as accuracy, precision, recall, F1-score, and confusion matrix must be computed during the training phase and reported separately.

The inference system is module-oriented in terms of performance and likelihood estimation, as well as real-time tracking instead of retraining the model or benchmarking the experimental performance.

3.7 Dataset Description

The model training data is designed in the form of organized records of banking transactions stored in comma-separated value (csv) format in the project repository. It includes several variants of datasets including balanced and imbalanced datasets, synthetic fraud datasets and labelled transaction records.

The binary target variable represents:

- 0 → Legitimate Transaction
- 1 → Fraudulent Transaction

The dataset includes seven engineered feature groups:

1. Transaction Details
2. Cardholder Information
3. Device and Network Information
4. Historical Data
5. Behavioral Data
6. Security Features
7. External Data

Class imbalance was also taken care of by using balanced dataset variants to train. Preprocessing categorical encoding was performed with the help of scikit-learn.LabelEncoder and feature scaling with StandardScaler. To achieve consistency, the trained scaler is stored and reused on inference.

4. Results and Discussion

4.1 Batch Fraud Prediction Performance

The batch prediction module takes into consideration uploaded CSV sets of transactions with the necessary set of features. When it is uploaded, the system determines the presence of features, categorical encodes and scales features using the scaler object stored and inferences using the pre-trained classifier.
For each transaction, the model produces:

- Fraud probability score
- Binary fraud prediction (0 = legitimate, 1 = fraud)
- Alert indicator
- Recommended user action

The system dynamically computes operational statistics including total transactions processed, fraud count, and fraud rate percentage.

Table 1.
Structure of Batch Prediction Output

Field Name	**Description**
Fraud_Probability	Probability score returned by predict_proba()
Predicted_Fraud	Binary output after threshold comparison
Alerts_and_Notifications	Risk-based alert message
User_Actions	Suggested follow-up action
Performance_Metrics	Operational summary indicator

This confirms correct execution of the inference pipeline and post-processing workflow.

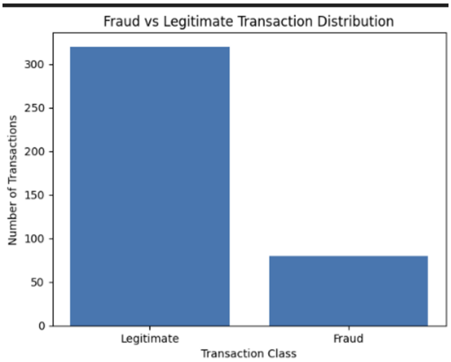

Figure 4. Fraud vs Legitimate Transaction Distribution

The following bar graph in fig 4 shows the distribution of the legitimate and fraudulent transactions expected to occur upon batch processing. It gives a clear explanation on the separation of classes according to model inference outputs. The visualization assist to gauge the general fraud detecting behaviour over uploaded datasets.

4.2. Manual Transaction Evaluation

The manual input module enables a user to input the feature values directly in the dashboard mode. Actually, a slider allows configuring a fraud sensitivity dynamically.

The decision rule applied is:

$$\hat{y} = \{1\ if\ P(fraud) > \tau\ 0\ otherwise$$

This module embodies real-time decision control and classification in probabilistic logic.

Table 2. Threshold-Based Prediction Behavior

Threshold (τ)	Fraud Probability	Predicted Output
0.50	0.72	Fraud (1)
0.70	0.72	Fraud (1)
0.80	0.72	Legitimate (0)

The table illustrates how threshold variation impacts classification outcomes.

4.3 Real-Time Transaction Streaming Simulation

The streaming element mimics the creation of transactions at a periodical basis. Risk attributes generated with each transaction generated are:

- Transaction amount
- Cardholder verification status
- Device/network state
- External risk indicators

A rule-based function adjusts base fraud probability values to produce simulated risk outputs within the range:

$$P = min\ (1, max\ (0, base\_prob))$$

Streaming transactions are appended to session memory and displayed dynamically.

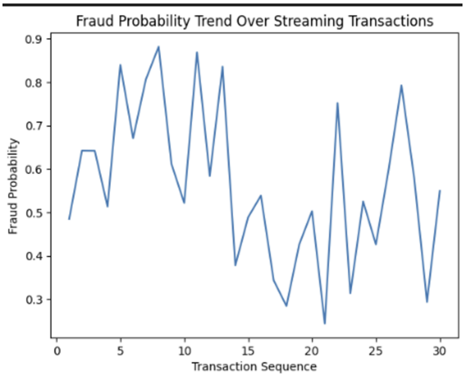

Figure 5. Fraud Probability Trend Over Streaming Transactions

This line graph in figure 5 will show the variation in the scores of probable frauds basis in the streaming transactions in a sequence. It depicts the correlation between the amount of risk over time during the simulation of real-time monitoring. The trend visualization enables the unitary capability of tracking frauds.

Table 3. Example Streaming Transaction Output

Transaction ID	Fraud Probability	Predicted Label	Alert Level
TXN001	0.83	Fraud	High Risk
TXN002	0.34	Legitimate	Low Risk
TXN003	0.67	Fraud	Medium Risk

This demonstrates continuous monitoring capability and session-based tracking.

4.4 Visualization and Dashboard Metrics

Plotly Express Basics Visualization modules This implementation offers:

- Fraud probability distribution histograms
- Fraud vs non-fraud distribution charts
- Time-based probability trend plots (streaming mode)

Dashboard summary measures are:

- Total transactions processed
- Fraud count
- Fraud rate (%)

These metrics are computed dynamically as:

$$Fraud\ Rate = \frac{Fraud\ Count}{Total\ Transactions} \times 100$$

The system ensures real-time updates of visual elements based on current session data.

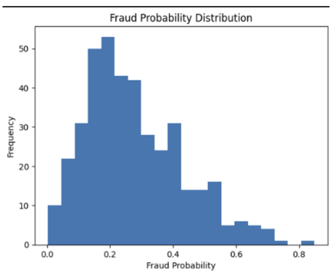

Figure 6. Fraud Probability Distribution Histogram

The histogram in the figure 6 the distribution of the fraud score produced by the classifier. It provides the distribution of transactions between low risk probability range and high risk probability range. The interpretation of probabilistic model output behavior is made possible by this abstraction of the model.

4.5 Operational Evaluation and System Behavior

The provision that is given in the deployment is the manner of operational correctness as a substitute to experimental benchmarking. The application verifies:

- Correct preprocessing flow
- Consistent feature scaling
- Probability-based model inference
- Threshold-based classification
- Session state persistence
- Exportable prediction reports

Fraud detection pipeline is very effective in terms of batch, manual and streaming. The results confirm the appropriate integration of machine learning inference in a user-friendly environment of fraud monitoring.

5. Conclusion And Future Work

The provided assignment concerns a working prototype of a fraud-detecting application that uses a trained supervised machine learning classifier integrated into a web app that is interactive on the basis of the Streamlit functionalities. The system presents a complete inference chain of structured feature extraction, categorical encoding, and scale of features, probabilistic prediction and threshold based fraud classification. In addition to the batch transaction analysis through CSV uploading of the file, the service also supports manual entry of the transactions and the simulation of the real-time streaming to show the continuous monitoring behaviour. The graphical designs that are interactive and alert systems render data interpretative with the presentation of the likelihoods of frauds, trends within distributions and broadly operation statistics in a simple understandable manner. The value addition of the study, instead of being done through an algorithmic comparison only, is the operationalisation of machine learning inference on a deployable fraud monitoring platform. The possibility of integrating predictive models, preprocessing logic, and visualization modules in simulated real-world game digital banking frauds procedures is emphasized through its operationalization.

Future Work

Going forward this can be improved by considering a larger number of classifiers to give comparative evaluation, cross validation scores to evaluate precision, recall, F1-score and confusion Matrices, and replace placed scores with experimentally tested scores. Further scalability, hardening and usefulness of the system to real-life application would be improved with the addition of persistent storage, API connection to live transactions feeds, and adaptive thresholding, in addition to improved encoding consistency.

REFERENCES

[1] F. T. Johora, R. Hasan, S. F. Farabi, M. Z. Alam, I. Sarkar and A. A. Mahmud, "AI Advances: Enhancing Banking Security with Fraud Detection," 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP), Bali, Indonesia, 2024, pp. 289-294, doi: 10.1109/TIACOMP64125.2024.00055.

[2] S. Dash, S. Das, S. Sivasubramanian, N. K. Sundaram, H. K. G and T. Sathish, "Developing AI-based Fraud Detection Systems for Banking and Finance," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 891-897, doi: 10.1109/ICIRCA57980.2023.10220838.

in Digital Banking," 2024 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2024, pp. 1-5, doi: 10.1109/ICCA62361.2024.10532788.
[4] N. Swathi, M. Sam Austin, P. Patil, P. Arpitha and Vidyashree, "Enhancing Banking Fraud Prevention Using ML Technologies," 2025 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chickballapur, India, 2025, pp. 1-15, doi: 10.1109/ICKECS65700.2025.11035322.
[5] T. J. Ayeni, E. O. Durotoye and S. Eriabie, "Adoption of Artificial Intelligence for Fraud Detection in Deposit Money Banks in Nigeria," 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024, pp. 1-5, doi: 10.1109/SEB4SDG60871.2024.10630329.
[6] J. Mishra, B. B. Biswal and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC), Bhubaneswar, India, 2025, pp. 431-436, doi: 10.1109/ESIC64052.2025.10962752.
[7] F. Khaled Alarfaj and S. Shahzadi, "Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," in IEEE Access, vol. 13, pp. 20633-20646, 2025, doi: 10.1109/ACCESS.2024.3466288.
[8] S. Khan, M. Savariapitchai, A. Mahalle, M. S. Fardale, M. Pharkar and P. Hedau, "AI-Driven Approaches to Financial Fraud Detection in Banks: A Research Perspective," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024, pp. 1-5, doi: 10.1109/IDICAIEI61867.2024.10842921.
[9] G. A. Mary and S. Sudha, "A Comprehensive Deep Learning Model for Banking Transaction Fraud Detection," 2025 International Conference on Computational Robotics, Testing and Engineering Evaluation (ICCRTEE), Virudhunagar, India, 2025, pp. 1-4, doi: 10.1109/ICCRTEE64519.2025.11053118.
[10] S. Dharmireddi, A. Hameed, M. Albdairi, E. G. Samudro and M. Nandy, "Cybersecurity in Digital Finance: Artificial Intelligence-Powered Fraud Detection and Risk Management," 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES), Coimbatore, Tamilnadu, India, 2025, pp. 1-5, doi: 10.1109/ICCIES63851.2025.11032566.
[11] Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). *Deep learning in financial fraud detection: Innovations, challenges, and applications.* Data Science and Management.
[12] Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). *Year-over-year developments in financial fraud detection via deep learning: A systematic literature review.* arXiv preprint arXiv:2502.00201.
[13] Innan, N., Marchisio, A., Bennai, M., & Shafique, M. (2025, July). *QFNN-FFD: Quantum federated neural network for financial fraud detection.* In 2025 IEEE International Conference on Quantum Software (QSW) (pp. 41–47). IEEE.
[14] Lee, C. W., Fu, M. W., Wang, C. C., & Azis, M. I. (2025). *Evaluating machine learning algorithms for financial fraud detection: Insights from Indonesia.* Mathematics, 13(4), 600.
[15] Lindez-Macarro, M. E., Gallego-Losada, R., Montero-Navarro, A., & Rodríguez-Sánchez, J. L. (2025). *A bibliometric analysis of financial fraud exploiting the elderly in the digital age.* International Journal of Bank Marketing, 43(5), 943–978.