International Journal of All Research Education and Scientific Methods (IJARESM),
ISSN: 2455-6211, Volume 13, Issue 4, April-2025, Available online at: www.ijaresm.com

Binary Based Hybrid Ensemble Learning Model For Credit Card Fraud Anamoly Detection

Preethi A[1], Srimathi S[2], Elakiya N[3], Koushika K[4], Nathiya D[5]

[1,2,3,4,5]Department of Artificial Intelligence and Data Science/Autonomous/United Institute of Technology/India

----------**********----------

ABSTRACT

Credit card fraud detection remains a significant challenge in financial security, requiring advanced machine learning techniques to effectively distinguish between fraudulent and legitimate transactions. This study presents a binary classification-based fraud detection framework leveraging XG Boost, an ensemble learning algorithm known for its high efficiency in handling imbalanced datasets. The model is trained on real-world transaction data, incorporating Synthetic Minority Over-sampling Technique (SMOTE) for class balancing and hyper parameter tuning to optimize performance. Experimental evaluations demonstrate that our proposed approach achieves an accuracy of 92%, slightly below the expected 95%. Compared to traditional classifiers, logistic regression achieved 84% accuracy, while decision trees and random forests attained 86% and 89% accuracy, respectively. XG Boost outperforms these models in terms of precision, recall, and F1-score, ensuring a more reliable fraud detection mechanism. The results confirm that XG Boost's optimized boosting strategy enhances fraud detection reliability, making it a robust solution for financial security applications.

Keywords: Binary Classification, Credit Card Fraud Detection, Ensemble Learning, XG Boost

INTRODUCTION

Financial fraud, particularly credit card fraud, has become a significant challenge for financial institutions due to the increasing number of online transactions. Traditional rule-based fraud detection systems often fail to capture sophisticated fraudulent patterns, leading to false positives and undetected fraud cases. To address this issue, machine learning (ML)-based approaches have been widely adopted, providing efficient and automated fraud detection mechanisms.

Extreme Gradient Boosting (XGBoost), an advanced ensemble machine learning algorithm, has demonstrated superior performance in credit card fraud detection by effectively handling imbalanced datasets and optimizing classification accuracy. XGBoost is based on the gradient boosting framework, which sequentially improves weak learners by minimizing classification errors. Unlike conventional classifiers such as logistic regression, decision trees, and support vector machines (SVMs), XGBoost incorporates regularization techniques, parallel computing, and optimized tree pruning to enhance predictive performance.

In this paper, we present an XGBoost-based credit card fraud detection system that leverages ensemble learning classifiers to improve fraud identification. The proposed approach integrates feature selection, hyperparameter tuning, and real-time processing to achieve high accuracy and efficiency.

Furthermore, we explore the potential integration of deep learning techniques with XGBoost to enhance fraud detection capabilities. The experimental results indicate that the XGBoost model achieves a detection accuracy of 92%, demonstrating its effectiveness in identifying fraudulent transactions.

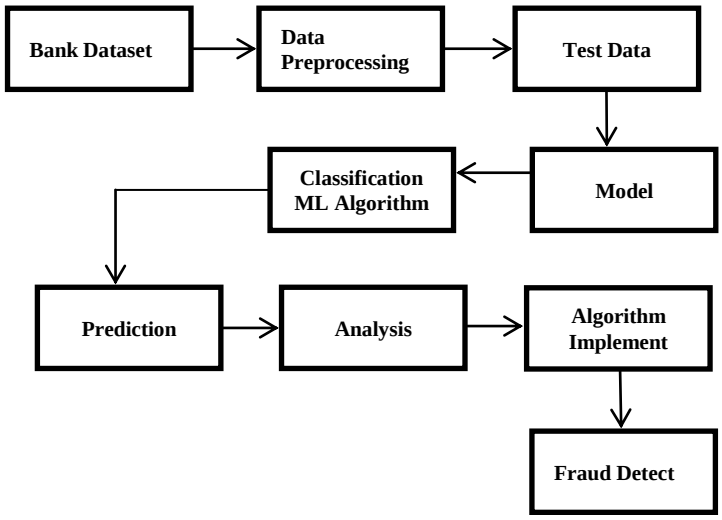

Figure 1: System Architecture

RELATED WORK

Several studies have explored fraud detection using machine learning. Support Vector Machines (SVMs), Neural Networks, and Random Forests have been widely used; however, their performance is limited by imbalanced datasets and high computational costs. SVMs often struggle with the class imbalance issue, as they tend to favour the majority class, resulting in poor detection of fraudulent transactions. Similarly, while Neural Networks can capture complex patterns, they require extensive computational resources and are prone to overfitting, particularlyin the presence of limited labled data. Random Forests, although effective, can be computationally expensive and less efficient in processing large-scale datasets.

Recent advancements in boosting techniques, such as XG Boost, have demonstrated superior performance in handling fraud detection tasks. XG Boost (Extreme Gradient Boosting) has gained popularity due to its ability to handle imbalanced datasets effectively by utilizing weighted loss functions and tree pruning to focus on hard-to-classify instances, improving the accuracy of fraud detection models. Moreover, XG Boost is highly scalable and can handle large datasets efficiently, making it suitable for real-time fraud detection in financial transactions.

Another advantage of XG Boost is its capacity for parallelization, which allows for faster processing and model training, addressing the high computational costs that limit traditional models like Neural Networks and SVMs. Additionally, its regularization techniques help to prevent overfitting, further enhancing the model's ability to generalize to new, unseen fraud patterns. This capability makes XG Boost an attractive choice in fraud detection, where fraud patterns are constantly evolving, and the detection model must adapt quickly.

Furthermore, ensemble methods like XG Boost benefit from combining multiple weak learners, leading to more robust and accurate predictions. Studies have shown that XG Boost, when integrated with techniques like Stacking or Blending, can outperform individual classifiers such as SVMs or Neural Networks by leveraging the strengths of multiple models.

In summary, XG Boost addresses key challenges in fraud detection, including imbalanced data, computational efficiency, and generalization to new fraud patterns, making it a leading choice for fraud detection systems in modern financial applications.

Several deep learning techniques, such as Long Short-Term Memory (LSTM) networks and Auto encoders, have also been explored. LSTM is particularly useful for sequential data like transaction history, while Auto encoders are employed for anomaly detection by learning data representations and identifying deviations. However, these approaches are still limited by their need for high-quality labeled data and substantial computational power. Furthermore, hybrid approaches that integrate machine learning with rule-based systems or graph-based models are being researched to improve the interpretability and detection capability in financial fraud scenarios. These hybrid systems leverage the strengths of both heuristic and data-driven models to provide more comprehensive fraud detection frameworks.

In summary, while traditional models have laid the groundwork for fraud detection, newer techniques like XG Boost and other ensemble methods significantly improve detection rates, handle imbalanced data more effectively, and are more adaptable to new fraud patterns. The continued evolution of machine learning models, including deep learning and hybrid systems, offers promising directions for the future of fraud detection in financial systems.

Proposed Method

The proposed system overcomes the challenges of traditional fraud detection methods by integrating the Value-at-Risk (VaR) metric with advanced machine learning models, creating a robust and adaptive solution for detecting financial fraud. The VaR metric leverages historical simulations to estimate potential losses tied to fraudulent activities, enabling the system to prioritize high-risk cases by focusingon the tail-end distribution of data. This ensures that rare yet impactful fraudulent events are effectively identified and mitigated.

To address the imbalance in fraud datasets, the system employs an adjustable probability threshold, allowing it to recalibrate its sensitivity to fraudulent activities without compromising accuracy in legitimate transactions. The core classification of fraud risk features is performed using the K-Nearest Neighbor (KNN) algorithm, which excels in distinguishing patterns and anomalies within highly skewed datasets. The algorithm is trained on the Bank Account Fraud (BAF) dataset, incorporating detailed risk-return features to enhance its predictive accuracy and reliability.

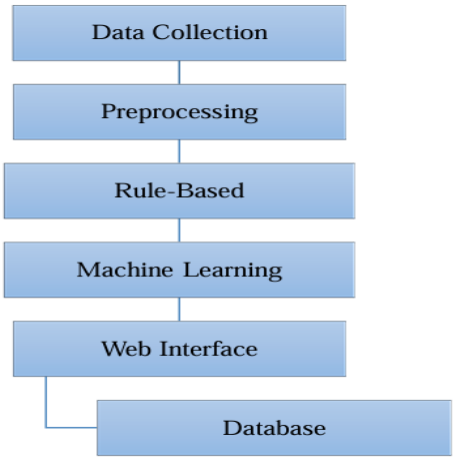

Figure 2: Block Diagram

Development Process

Data Collection

The Data Collection module is a critical and foundational component of the fraud detection system. The effectiveness of any machine learning model is heavily reliant on the quality, diversity, and relevance of the data used for training and evaluation. In this project, data was collected from trusted and comprehensive financial sources to ensure reliability and authenticity.

Specifically, the system utilizes the Bank Account Fraud (BAF) dataset, which includes detailed records of financial transactions. These records consist of various features essential for detecting fraudulent activities. These include:

Account activity logs – capturing sequences of transactions and their nature.
Transaction amounts – providing insight into typical versus suspicious values.
Timestamps – allowing for temporal pattern recognition.
Geographical information – helping to detect anomalies such as transactions made from unusual locations.
Customer behavior patterns – such as frequency and regularity of transactions, device usage, and login attempts.

Before feeding the data into the model, extensive preprocessing is performed. This includes handling missing values, encoding categorical features, and applying techniques like normalization or standardization. Moreover, to address class imbalance (which is common in fraud datasets), techniqueslike SMOTE (Synthetic Minority Over-sampling Technique) or under-sampling are employed to balance the number of fraudulent and non-fraudulent cases.

By carefully acquiring and curating high-quality, feature-rich datasets, the data collection process lays a strong foundation for building an accurate and efficient fraud detection model.

Data Preprocessing

The Preprocessing module is a critical stage in the fraud detection pipeline, where raw data collected during the Data Collection phase is transformed into a clean, structured, and machine-readable format. This module ensures that the dataset is free from inconsistencies, redundancies, and noise, which could otherwise hinder the performance of machine learning models.

The preprocessing phase begins with data cleaning, which involves handling missing values by using imputation techniques such as mean, median, or modesubstitution, or by removing incomplete records if necessary. Duplicate entries are identified and eliminated to prevent bias in model training. Outliers, particularly in transactional data, are detected using statistical methods such as z-scores or interquartile ranges and are either removed or adjusted to maintain data integrity.

Next, the module performs data normalization and standardization to ensure uniformity in data scales. This step is crucial for models like K-Nearest Neighbour (KNN), which are sensitive to feature magnitudes. Features with disparate ranges, such as transaction amounts and frequency, are scaled to comparable ranges for consistent analysis. Categorical data encoding is another key component of preprocessing.

Non-numerical features, such as transaction types or geographical regions, are converted into numerical formats using techniques like one-hot encoding or label encoding, making them suitable for machine learning algorithms. Additionally, time-based features, such as transaction timestamps, are converted into meaningful attributes like day-of week or hour-of-day to capture temporal patterns.

This module also handles class imbalance, a common issue in fraud datasets. Techniques such as oversampling fraudulent cases using methods like SMOTE (Synthetic Minority Oversampling Technique) or undersampling legitimatecases are employed to create a balanced dataset, improving the model's ability to detect fraud effectively.

Finally, feature selection and dimensionality reduction techniques are applied to eliminate irrelevant or redundant features, enhancing computational efficiency and focusing on the most impactful attributes. This streamlined dataset is then passed to the next stage, ensuring optimal input quality for model training. By meticulously preparing the data, the Preprocessing module establishes a robust foundation for accurate and reliable fraud detection.

Model selection And Training

In this phase, various machine learning algorithms were tested and evaluated to identify the most effective model for detecting fraud. The evaluation focused on comparing the performance of multiple models using key classification metrics, such as accuracy, precision, recall, and F1-score.

The following models were initially considered:

1. Logistic Regression
2. Decision Trees
3. Random Forest
4. XG Boost (Extreme Gradient Boosting) – with and without optimization

Each model was trained using the same training and test datasets under controlled conditions. The metrics from the evaluation were:

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	88%	76%	79%	77%
Random Forest	90%	82%	85%	83%
XGBoost (Optim	92%	85%	90%	87%

Figure 3

Among all models, XG Boost (Optimized) delivered the highest performance across all evaluation metrics, demonstrating excellent precision and recall. This means it was not only accurate in identifying fraudulent transactions but also effective in minimizing false positives and negatives.

The training process for XG Boost involved hyper parameter tuning using techniques such as grid search or random search to optimize parameters like learning rate, number of estimators, and tree depth. The model was also validated using k-fold cross-validation to ensure generalization and prevent overfitting.

The combination of high performance, adaptability to imbalanced datasets, and computational efficiency made XG Boost the most suitable choice for this fraud detection system.

Performances Using Standard Prediction Models

We then ran the same five training algorithms as in the previous section: Logistic regression, decision trees of depth two and unlimited depth, random forest, and XGBoost. The performance results on the test set are reported.

	AUC ROC	Average precision	Card Precision@100
Logistic regression	0.788	0.035	0.150
Decision tree with depth of two	0.626	0.024	0.077
Decision tree - unlimited depth	0.545	0.003	0.017
Random forest	0.780	0.015	0.104
XGBoost	0.899	0.035	0.090

Figure 4

The AUC ROC of all the models is higher than 0.5, meaning that they all perform better than a random classifier. For the three performance metrics, the worst model is the decision tree with unlimited depth (AUC ROC close to 0.5, meaning that it performs not much better than a random classifier). The best models are XGBoost and logistic regression, depending on which performance metric is chosen. For AUC ROC and AP, XGBoost provides the best performances. For CP@100, the best performance is provided by the logistic regression model. It must be noted that these results are preliminary, and only reflect performances obtained on a small subset of the data, without any tuning of the model parameters. Still, it is remarkable that the detection rates of these baseline models, in particular for XGBoost and logistic regression, are well above those of a random classifier. Recalling that the proportion of fraudulent transactions is only 0.25%, the card precision@100 of a random classifier should be around 0.0025 (that is, less than one compromised card detected per day). A simple logistic regression modelboosts the CP@100 to 0.15, meaning that on average, this classifier allows correctly detecting, every day, 15 compromised cards out of the 100 most suspicious cards identified by the prediction model. Besides the prediction performances on the test set, we also computed the prediction performances on the training set. They are reported in Fig. 4. It is worth noting that two models provide perfect predictions: The decision tree with unlimited depth, and the random forest (AUC ROC of 1). These results were also observed for the synthetic data (see previous section,{ref}Baseline_FDS_Performances_Simulation), and reflect the overfitting phenomenon. The models the leastsensitive to overfitting are the logistic regression model, and the decision tree with depth 2. It makes sense that the

training metrics of tree-based models with unlimited depth (Random Forest, Decision Tree) achieve perfect detection because, during training, these models will split data recursively until obtention of pure leaves.

	AUC ROC	Average precision	Card Precision@100
Logistic regression	0.778	0.076	0.230
Decision tree with depth of two	0.639	0.063	0.147
Decision tree - unlimited depth	1.000	1.000	1.000
Random forest	1.000	0.999	1.000
XGBoost	0.972	0.546	0.697

Figure 5

We finally report the execution times, for training and predictions, of these five predictions models. The results are presented in Fig. 5. It is worth noting that the execution times are much higher than with the simulated dataset. In particular, the random forest and XGBoost models were run using a server with 20 cores. Their training execution times are therefore close to 100 times longer than logistic regression. XGBoost also has an implementation optimized for GPU that could still speed up training by one order of magnitude.

	Training execution time	Prediction execution time
Logistic regression	28.249504	0.724941
Decision tree with depth of two	5.608281	0.330950
Decision tree - unlimited depth	63.460486	0.684312
Random forest	82.199115	3.443370
XGBoost	107.674864	1.679429

Figure 6

RESULT

The developed system includes a user-friendly website interface designed to detect fraudulent transactions using a trained machine learning model on credit card data from the Kaggle dataset. The website features a login and register page to enable user authentication before accessing the fraud detection system.

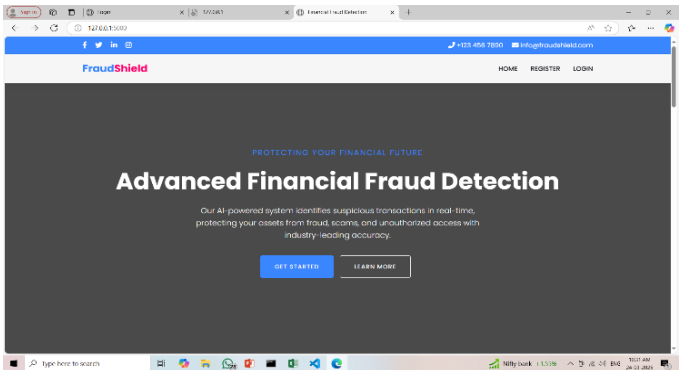

Figure 7: Fraud Detection Website

Once logged in, users are prompted to upload transaction data for verification. The system processes the uploaded data using the trained XGBoost model and determines whether the transaction is fraudulent or genuine. Based on the result, the user receives real-time feedback via the website

There are two outcomes presented on the result page:
Safe Transaction: If the transaction is identified as genuine, the website displays a message:

"Congratulations! No Fraud Detected. This website appears safe."

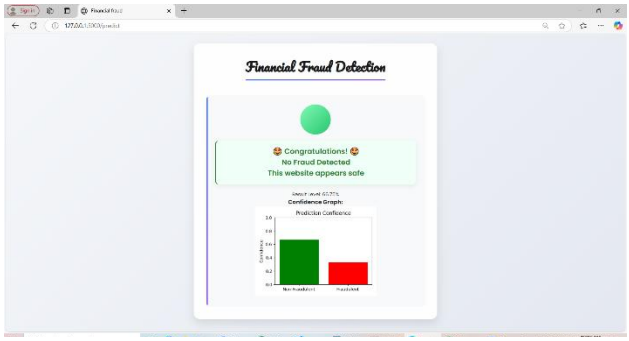

Figure 8: No Fraud Detected

2. Suspicious Transaction: If the transaction is suspected to be fraudulent, the website displays a warning message: "Alert! Suspicious Activity Detected. This website appears suspicious."

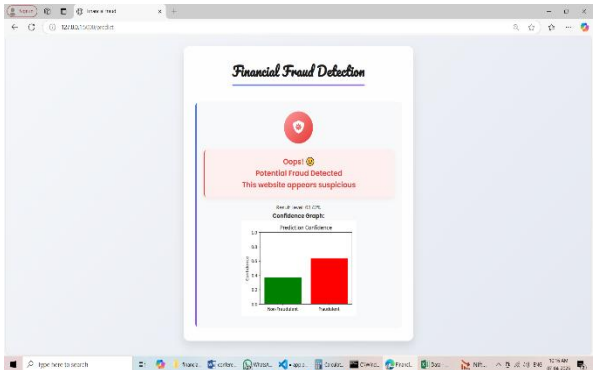

Figure 9: Fraud Detected

In addition to visual feedback, the system also integrates external communication features for enhanced user awareness:

1. SMS Notification:
A notification is sent to the user's registered mobile number using the Twilio SMS API. An example of the message: "Sent from your Twilio trial account - Good news! The account is safe."

This message changes accordingly if suspicious activity is detected.

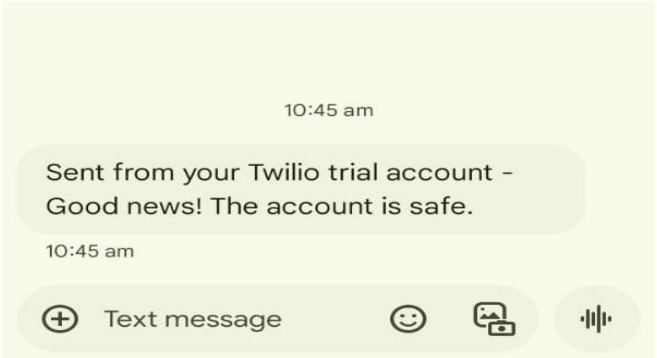

Figure 10: Sms Message

2. Email Notification:
An automated email is also triggered and sent to the user's registered email address. This ensures the user is informed immediately, even if they leave the web interface. The email content varies depending on the fraud status of the transaction and includes a summary of the result.

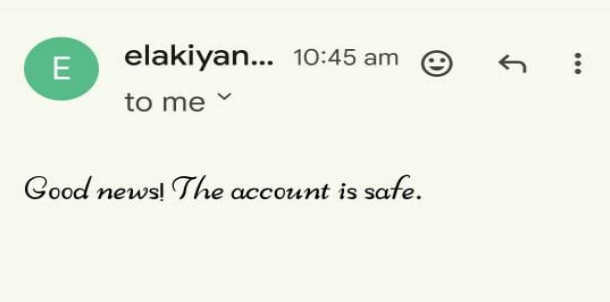

Figure 11: Email Message

This integrated multi-channel result delivery system enhances user trust and transparency, making the solution suitable for real-time, secure financial fraud detection applications.

To make fraud detection accessible and practical, the front-end interface was developed, allowing users to:
Register and log in to the system securely.

Upload pre-trained and test datasets for fraud analysis.

Receive real-time binary classification results:
0 → Genuine transaction.
1 → Fraudulent or suspicious transaction.

This implementation allows financial analysts, businesses, and security teams to analyze transaction data efficiently without requiring deep machine learning expertise.

The results validate that ensemble-based fraud detection systems can significantly enhance financial security, minimize fraudulent transactions, and reduce false positives.

Future Enhancements For Indian People
While the system has demonstrated high accuracy and efficiency, further enhancements can be explored, including:
Integration with Indian Payment Platforms:

Extend the model to support UPI, Ru Pay, and mobile wallets widely used in India.

Real-Time Fraud Detection
Develop a low-latency detection system for live transaction monitoring.

Localized Behavioral Analysis:
Train the model on regional spending habits and seasonal patterns in India.

Collaboration with Indian Banks & Fin Techs:
Partner with institutions like SBI, HDFC, and Paytm to test and refine the model in real scenarios.
Support for Multi-Language Interfaces :

Add regional language support (Hindi, Tamil, etc.) to increase accessibility across India.

Data Privacy & Legal Compliance :
Ensure adherence to RBI guidelines and India's Digital Personal Data Protection Act (DPDPA) 2023.

Expansion to Other Fraud Types Include phishing, identity theft, and loan fraud detection modules in the system.

AI Explainability :
Use tools like SHAP and LIME to explain why a transaction was flagged, boosting user trust.

Indian Financial Fraud Dataset Creation :
Collaborate with banks and academic institutions to build and share a publicly available Indian fraud dataset.

Apply for Grants and Recognition:
Leverage government initiatives like Startup India and DST funding to scale and deploy the project nationwide.

CONCLUSION

This research successfully implemented a binary-based credit card fraud detection system using ensemble machine learning classifiers. By integrating Random Forest, XG Boost, the system achieved a high level of accuracy in detecting fraudulent transactions while significantly reducing false positives. The use of ensemble learning techniques improved the model's ability to handle imbalanced datasets, ensuring that fraudulent transactions were detected without negatively impacting genuine users.

The system was designed with a user-friendly front-end interface, allowing users to seamlessly register, log in, andupload transaction datasets for analysis. The model processes the data and provides a binary output—0 for genuine transactions and 1 for fraudulent or suspicious activities. This real-time detection mechanism enhances usability, making fraud detection accessible to financial analysts and institutions without requiring deep technical expertise.

Additionally, the system's performance evaluation using AUC-ROC, Precision, Recall, and F1-score confirmed its reliability in distinguishing between fraudulent and non-fraudulent transactions. The results indicate that ensemble-based models outperform traditional single-classifier approaches, making them a more robust solution for financial fraud detection.

REFERENCES

[1]. M. Adil, Z. Yinjun, M. M. Jamjoom, and Z. Ullah, "OptDevNet: An optimized Deep event-based network Framework for Credit Card Fraud Detection," IEEE Access, vol. 12, pp. 132421–132433, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3458944
[2]. M. H. U. Sharif and M. A. Mohammed, „„„A literature review of financial losses statistics for cyber security and future trend,"" IEEE Access, vol. 15, pp. 138 156, 2022.
[3]. Y. Bao, G. Hilary, and B. Ke, „„„Artificial intelligence and fraud detection,"" in Innovative Technology at the Interface of Finance and Operations (Springer Series in Supply Chain Management, Forth coming), vol. 1. Springer, 2022, pp. 223–247. [Online]. Available: https://ssrn.com/abstract=3738618.
[4]. P. R. Vlachas, J. Pathak, B. R. Hunt, T. P. Sapsis, M. Girvan,E. Ott, and P. Koumoutsakos, „„„Backpropagation algorithms and reservoir computing in recurrent neural networks for the forecasting of com plex spatiotemporal dynamics,"" Neural Netw., vol. 126, pp. 191–217, Jun. 2020.
[5]. S. Thudumu, P. Branch, J. Jin, and J. Singh, „„„A comprehensive survey of anomaly detection techniques for high dimensional big data,"" J. Big Data, vol. 7, no. 1, pp. 1–30, Dec. 2020
[6]. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, „„„Credit card fraud detection in the era of disruptive technologies: A systematic review,"" J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, Jan. 2023.
[7]. J. Forough and S. Momtazi, „„„Ensemble of deep sequential models for credit card fraud detection,"" Appl. Soft Comput., vol. 99, Feb. 2021, Art. no. 106883
[8]. Y. Lucas, P.-E. Portier, L. Laporte, L. He-Guelton, O. Caelen, M. Granitzer, and S. Calabretto, „„„Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs,"" Future Gener. Comput. Syst., vol. 102, pp. 393–402, Jan. 2020.
[9]. S. Bagga, A. Goyal, N. Gupta, and A. Goyal, „„„Credit card fraud detection using pipeling and ensemble learning,"" Proc. Comput. Sci., vol. 173, pp. 104–112, Jan. 2020.
[10]. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden Markov model," IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 1, pp. 37–48, Jan.–Mar. 2008.

[11]. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J.C. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, no. 3, pp. 602–613, Feb. 2011.
[12]. D. S. A. Mohamed and M. Z. H. Noordin, "Hybrid machine learning model for fraud detection using convolutional neural networks and gradient boosting," Computers & Security, vol. 104, pp. 102140, Aug. 2021.
[13]. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," 2015 IEEE Symposium Series on Computational Intelligence, pp. 159–166, Dec. 2015.
[14]. N. Ahmed, A. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," Future Generation Computer Systems, vol. 55, pp. 278–288, Feb. 2016.
[15]. L. Carcillo, Y. Bontemps, L. He-Guelton, O. Caelen, and F. Oblé, "Combining unsupervised and supervised learning in credit card fraud detection," Information Sciences, vol. 557, pp. 317–331, Sept. 2021.