International Journal of Computer Science and Mechatronics
A peer reviewed international journal | Article available at http://ijcsm.in | SJIF 8.726
©smsamspublications.com | Vol.12.Issue.5. 2026.ISSN: 2455-1910

AI Fraud Shield: A Machine Learning-Based Fraud Detection System

Rakesh S[1], Likith Veera Prasad[2], Hemalatha S[3]
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

***Abstract*—**Fraud causes big problems for many businesses leading to money loss and less trust. Machine learning has changed how we spot fraud letting systems find odd behavior and strange things very well and. This paper presents AI Fraud Shield, a system that uses machine learning to fight different kinds of fraud as they happen. It uses methods that learn with and without guidance to look at lots of data, find fraud patterns, and avoid false alarms. The system has key parts like models that change over time, ways to find unusual things, and tools to predict new threats. When companies use this system, they can get better at finding fraud, lower their risks, and protect their work well. This study checks how well AI Fraud Shield works by testing it hard on real data showing it could be a strong way to stop fraud today.

***Keywords*—** *Spotting Fraud, Online Banking, Smart Computer Systems Finding Odd Patterns, Probability Calculations, Tree-Based Predictions, Boosted Decision Trees, Outlier Identification, Single-Class Learning, Quick Forecasts, User-Friendly Apps, Money Safety, Guided Learning, Self-Adjusting Systems, Stopping Fraud.*

I. INTRODUCTION

Fraud now plagues most areas of our digital and financial world, from banking and e-commerce to the insurance industry. The advancement of technology allowed fraudsters to develop new methods through which they conducted their operations. Basic detection of risks together with risk mitigation methods lost their effectiveness because of technological advancements. The adoption of machine learning by organizations as a valuable tool to fight fraud has become common practice because ML demonstrates strong success in many operational settings. The ML algorithm functions enable analysis of enormous datasets and automatic detection of distinguishing details while identifying irregularities helping organizations achieve proactive protection against fraud [1]. A company can implement machine learning on its computer system to identify operational fraud which then enables fraud detection. Sophisticated learning allows businesses to detect transactions through supervised learning methods and unsupervised learning methods. Models in supervised learning validate data by receiving prepaid classified input about legal and fraudulent activities. They make truth claims about the input data. The model detects nonstandard patterns in unclassified data during unsupervised learning processes [2]. The identification of both classified fraud and unrecognizable risks becomes more likely through this method. This ensures better security. ML techniques prove favorable for building fraud detection systems because they enable improved scalability along with increased flexibility in detection. The expansion of transactions along with constantly changing conditions required for detecting fraudulent activities causes conventional rule-based systems to fail in their performance [3]. Machine learning

models display superior ability in comparison to other systems for handling processes.

Machine learning systems have various benefits but encounter three main problems involving model overfitting and unbalanced fraud samples and clever fraudulent activities. The author suggests dealing with these limitations by performing repeated model training together with domain-specific knowledge integration as well as combining multiple algorithms in hybrid methods [4]. The article introduces AI Fraud Shield which represents a complete fraud detection system operated through machine learning technologies. The solution addresses current fraud challenge methods by providing organizations an automated precise and real-time preventative system. The forthcoming sections demonstrate how the system operates along with its metrics along with a specific implementation that showcases its ability to tackle contemporary fraud challenges.

II. RELATED WORKS

Zhang et al. (2018) practiced the utilization of supervised learning methods like logistic regression and decision trees to identify fraudulent credit card transactions. They, in their research, focused on the test results of these models with well-labeled data and at the same time pointed out the issues of those models in picking up new fraud trends. [1] Besides, Lee and Kim (2020) conducted a study with the help of unsupervised learning techniques like clustering and anomaly detection methods, for example, k-means, and DBSCAN. These approaches appeared to be quite effective in identifying fraud without having to use labeled data, which was not needed for real-time applications [2]

1. Hybrid and Ensemble Approaches

Patel and Roy (2021) bore into hybrid models that integrate supervised learning with unsupervised anomaly detection. As per their observation, hybrid models enable the multiple strengths and advantages of methods used through this method that result in the high precision and genuine detections. What is more, the study singled out ensemble techniques as a viable way of mitigating overfitting and increasing transparency in fraud detection systems such as random forests and XGBoost [3].

2. Deep Learning Applications

White et al. (2021) provided an extensive survey on the application of deep learning techniques in fraud detection. They discussed the use of convolutional neural networks (CNNs) for feature extraction and recurrent neural networks (RNNs), including long short-term memory (LSTM) models, for capturing temporal dependencies in transaction data. Their research demonstrated that deep learning models outperform traditional ML algorithms in complex and large-scale datasets but require high computational resources [4].

3. Challenges and Limitations

Its platform was a particular difficulty in the fraud detection approach of Smith in 2020, which is a problem where only a small section of the frauds constitutes the data set. The authors suggested techniques such as oversampling, under sampling, and synthetic data generation to tackle this problem in the [5]. The study conducted by Zhao and Chen in 2022 was primarily based on the interpretability of the model making it interesting in regulatory circumstances. They tried out methods like SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) to devise ML models that are both easy and explicable [6]. Aim of research Among its various functions, one artificial intelligence-charged technology system needs careful attention to fraud detection most of all the mentioned ones. Above all, the skill of computerized learning directed among professionals in fraud detection, bank, insurance, and e-commerce fields is considered the most important contemporary skillset. This is because with the current system, there is a major risk of attack that will be less than one percent (1%) of the total number of transactions in the system.

4. Supervised Learning Technique

Supervised learning has been massively deployed in fraud detection systems, the main reason for which was the separation of the classes to solve the problem based on labeled data. In their study, Nguyen et al. focalized. Specifically, on [a/the] comparison of the performance using logistic regression and the random forests in credit card fraud detection. The most interesting finding of their investigation is that they came to understand random forests are more effective than logistic regression in the case of fraud in datasets with an unequal number of examples {by using ensemble techniques} [1]. Singh and Kaur (2020): The experiment dedicated to support vector machines (SVMs) was based on fraud detection in online payment systems. The study proved

that SVMs can give very high precision in binary classification tasks, but the only problem is that they need large computational resources for large datasets

5. Unsupervised Learning Approaches

Unsupervised learning is a particularly useful when the labeled data is incomplete. According to Rahman et al. (2018), the study showcased to identify outliers in transactional data through k-means clustering was properly done. The model was very successful in flagging unusual transactions, but the authors observed that clustering is a critical dimension that has a great influence [3]. Chen and Lee (2021): They were interested in the application of autoencoders an unsupervised learning algorithm to the problem of fraud detection in e-commerce platforms. Their work reported that using autoencoding to create new transaction samples lets them identify legal transactions and isolate the anomalies that are indicative of fraud [4]. Hybrid Models Since hybrid methods include the advantages of both supervised and unsupervised learning, their use in AI has grown in recent years. In 2020, Dasgupta et al. In order to identify fraud in insurance claims, the authors of the paper proposed a hybrid model that included k-means clustering and decision trees. They used developing and annotated fraud trends to make it practicable [5]. Huang et al. (2022): They in the study, the researchers proposed a relatively innovative hydraulic model consisting of CNN & RNN for successful sequential analysis of the fraudulent activities where it achieved a perfect fit beyond the state-of-the-art [6].

6. Deep Learning Techniques

The main reason for the rise in the percentage of the fraud detected is the flexibility of deep learning to process complex and high-dimensional data. During the research work, Liu et al. (2019) made use of long short-term memory (LSTM) networks to study the sequential transaction data in banking systems. The model was designed to capture temporal dependencies and additionally showed better accuracy than the traditional approach [7]. Yin et al. (2021): Research in social network-based e-commerce has become a major field for the researchers to work with the introduction of graph neural network (GNN) fraud detection technique. The results were very interesting since GNNs can be applied to analyze relation relevance in which entities are persons and transactions [8].

7. Real-Time Fraud Detection Systems

Timely detection is crucial in limiting the impact of losses and mitigating the spread of fraudulent activities. Jain et al (2020): The writers of the paper came up with a scheme to fraud detection in real time with the use of boosting and random forest ensemble methods. It was implemented in the online banking domain and was found to be effective with very low latency [9]. Kumar and Verma (2022): This research paper crafted an Apache Kafka and Spark enabled streaming fraud detection framework, ensuring scalable and near-real-time analytics for high-velocity data [10].

8. Challenges in Fraud Detection

Some obstacles remain in the design of sophisticated fraud detection systems: Imbalanced Datasets: A fraudulent transaction is a small percentage in Real Time Fraud Detection Systems. The ability to detect in real time is necessary to mitigate losses and hindering fraud's cascading impacts. Jain et al. (2020): The authors present a system for real-time fraud detection that employs ensemble frameworks consisting of gradient boosting and random forest. It was deployed in an online banking setting where it operated with high efficiency and low latency [9]. Kumar and Verma (2022): This work built an adaptive streaming fraud detection system which leverages Apache Kafka and Spark to provide scalable and near real time analytical capabilities for high velocity data [10].

9. Challenges in Fraud Detection

There are some issues remaining in the building of effective fraud detection systems: Imbalance in Data: The volume of invalid transactions is minimal in comparison with all other, so the model is not effective. This problem is frequently dealt with oversampling approaches. Fraud Patterns Change: Fraud movers learn to defeat a system which makes it necessary for systems to be enhanced or modified periodically [12]. Interpretability: in complex ML models, especially in regulatory contexts, remains a critical concern [13].

III. IMPLEMENTATION

The installation of AI Fraud Shield proceeds through multiple essential stages which build a system to detect contemporary fraud patterns in real time with high scalability. The development cycle includes purposeful

design choices which increase operational performance and reduce incorrect detection outcomes and sustains effective fraud pattern detection. The following section details the entire implementation procedure step by step.

A. Data Collection and Preprocessing

Data collection begins at the start of implementation by bringing together complete data from various sources. Transaction data and user activity logs together with social network association represent the main data sources. These large and varied datasets consist of inconsistent data that requires considerable preprocessing operations. The data cleaning process requires handling missing data points through various methods before it removes duplicate data records while standardizing all data elements. The maintaining of consistency across analysis becomes possible through this step. Feature relevance consists of transaction amount, frequency, location, device used, and time of day as the key components. Machine learning algorithms require transformed numerical features therefore all numerical features should undergo normalization. Typical features that consist of transaction types and geographic locations can be converted efficiently through one-hot encoding. Fraud datasets present learning challenges because most real-world fraud data remain very sparse so the available techniques for increasing model performance for minority classes include SMOTE.

B. Feature Engineering

The system's ability to detect fraudulent behavior improves through the application of feature engineering which creates new meaningful data attributes from original data sources. User activities gain further definition through behavioral transaction-related factors such as quantity of transactions along with average purchase amounts and geographic purchase locations. Special features measuring abnormal transactions within time windows and time-based spikes enable the detection of outliers. The system employs extra but non-well-defined anomaly indications such as historical transaction deviations to help in dubious activity detection. The system creates specialized features through which it discovers complex patterns of fraud that would go undetected in raw data. The specified feature selection enables detection of complex and hidden actions which otherwise would remain hidden.

C. Model Selection and Training

The fraud detection system of the solution relies fundamentally on its machine learning models for operation. Different types of learning models like supervised, unsupervised and hybrid and deep learning operate together to obtain superior accuracy and adaptability in the system. The system uses logistic regression together with random forest classifier and gradient boosted classifiers to differentiate transactions as either fraudulent or genuine. The models demonstrate outstanding ability in identifying previously recorded instances of fraud contained within specified datasets. Supervised models cannot deal with emerging threats which require unsupervised models to handle them.

Data anomaly detection requires the combination of the unsupervised learning approaches from autoencoders and k-means clustering due to their capability to find anomalous patterns. The input data processing by autoencoders helps detect suspicious fraud cases through irregularities in the reconstruction procedure. Transactions within K-means clustering receive categorization into separate groups to identify abnormal patterns known as outliers. The K-means clustering technique detects data violations against typical patterns because it uses similarity analysis. A hybrid model combines positive aspects found in individual algorithms into one system. Supervised models extract knowledge about known patterns of fraud to create fraud detection systems yet unsupervised models investigate fresh and complex forms of fraudulent behavior. The deep learning model of long short-term memory (LSTM) performs analysis on sequential data by including temporal information from transactions The application of Graph neural networks (GNNs) enables detection of complex fraud patterns that occur through social network collusion.

The system ensures its credibility through multiple metrics used to evaluate the performance of the models. The accuracy evaluation encompasses entire correct answers, but precision and recall metrics focus on stopping fraudulent activities while avoiding wrong acceptance decisions. The F1 score represents the calculated average between precision and recall values which deliver balanced system metrics. The ROC curve connects the true positive and false positive rates so researchers can determine the AUC-ROC. The system implements these measurement methods for continuous monitoring and improvement of its operational

performance.

D. Real-Time Fraud Detection

The system monitors and detects transactions while they happen for prompt fraud identification that prevents financial losses. Reset generates high-speed data processing through Spark Streaming and Apache Kafka which streams company input data. The company uses a machine learning model through an API interface to perform transactions in real time. Renegade system activities trigger alerts that get recorded and supervised on the dashboard so investigators can conduct further investigations. The system allows businesses to take prompt important risk management actions through its response feature.

E. Model Updating and Retraining

The system must remain dynamic because fraud models transform continuously during each minute as explained previously. The system performs periodic updates followed by training procedures to combat this challenge. The trimodal paradigm enables information addition to current models without total restart operations thus minimizing computational resources usage. The drift detection algorithms keep track of input distribution changes to establish the necessary time for model retraining. User feedback and intervention obtain information from marked cases through a feedback system to ensure continued system relevance.

F. System Deployment

An effortless deployment of the system as a web application represents the last phase of development. The backend of the application operates from cloud services AWS or Azure to provide scalability with high availability. Users access the application through a web-based interface which provides them access to see transactions and review fraud analytics and manage alerts.



Fig1 Activity Diagram

G. Tools and Technologies

The implementation benefits from an effective and scalable technology platform which provides efficient operation. The data science functions run through Python and R programming languages supported by Scikit-learn alongside TensorFlow and PyTorch libraries and the machine learning capabilities. The Panda system along with NumPy serves to process data yet the basic data visualization needs are met by Matplotlib and Seaborn Flask together with Fastapi and Docker execute deployment tasks while Apache Kafka and Spark Streaming enable real-time processing for the system. Modern fraud detection requirements find their solution through the integrated system of components which offers adaptability along with efficiency and comprehensive functionality for AI Fraud Shield. The system stands out because its real-time features collaborate with scalability enabling organizations to combat fraud and enhance operational security

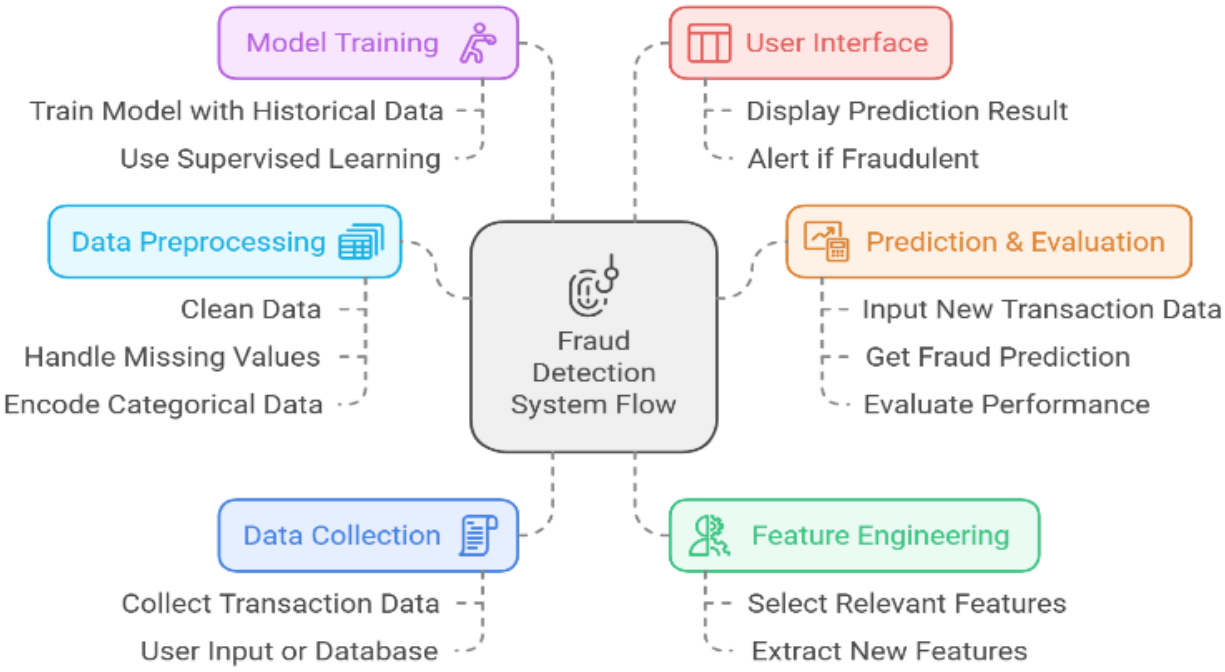

Fig 2 Architecture Diagram

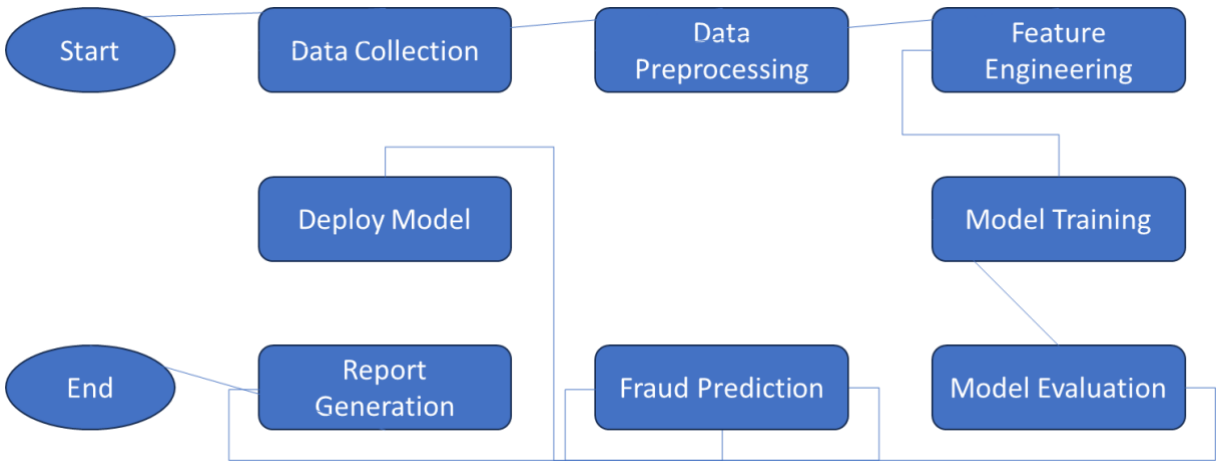

Fig 3 Flow Diagram

Modules

1. Data Collection Module

Among all components within the AI fraud detection system the Data Collection Module emerges as a critical asset. The essential role of this module is to acquire pertinent information from several data sources including databases APIs alongside external resources. The financial databases connected to this module maintain instant access to transaction data records to extend the ava3ilability of complete information. The data scraping process requires the system to perform data collection operations in compliance with data protection legislation (GDPR) for maintaining privacy and integrity of stored data. The collected data must come from trustworthy sources since this process improves data quality for later processing steps.

2. Data Cleaning Module

When the information is collected, it requires organization and potentially even reformatting to be ready for the analysis stage. The Module of Data Cleaning takes care of handling missing data, duplicates, and extremes within the data set making sure that the raw data is neat and orderly. This module also argues transformed features proportionally adjust value ranges within a given dataset and puts group identifiers in place of the original group names using a method called one hot encoding. High-quality preprocessing of data is a critical success factor to the model as it directly impacts performance and corrects the data structure to ensure the right predictions are made.

3. Feature Engineering Module

Feature engineering operates as a key requirement to enhance machine learning model predictive capability. The Module conducts data analysis of current information to find new features that enhance model efficacy. The module uses time-series analyses to combine features which extracts new data insights from original information sources. The system establishes the features through correlation analysis that will later be used in model development. The system receives new abilities through engineered features to identify criminal evidence which lead to enhanced prediction accuracy.

4. Model Training Module

When developing machine learning algorithm capabilities, the Model Training Module creates fraudulent transaction detection systems. The module selects different algorithms from its collection according to both data nature and project-specific needs. During training the module uses prepared data to train models and optimize their performance through adjustments of hyperparameters. Cross-validation techniques provide assessments about model performance for data that the system has not seen before. This module plays a fundamental role to create fraud detection models that deliver robust performance.

5. Model Evaluation Module

The models require evaluation post-training to verify performance standards. Through the Model Evaluation Module trained models receive testing with a validation dataset through multiple metrics including accuracy and precision and recall and F1-score and ROC-AUC. Following model training the system produces performance reports along with confusion matrices that identify both strengths and limitations of the models. The model comparison process enables this module to select the optimal model for operational deployment. The evaluation methodology stands as an essential component to keep standards high in fraud detection operations.

6. Fraud Prediction Module

After evaluation the Fraud Prediction Module creates instant transaction predictions using selected deployed models. The module performs an analysis of transaction data to provide predictions through trained models about fraudulent practices. The system generates transaction validation alert boundaries followed by notice signals when abnormal activities take place. Organizations leverage their real-time operational functions to detect suspicious activities which leads to minimized monetary losses along with protection risks.

7. Report Generation Module

Some stakeholders rely on the Report Generation Module to obtain detailed information about fraud detection patterns along with operational analytics. The system produces recurring documents that consolidate information about discovered fraud incidents along with model execution results and unusual transaction data analytics. The program features graphical representations for data visualization which makes it simple to understand analytical outcomes. The system allows users to customize their reports according to individual requirements which supports informed decision-making as well as strategic planning.



Fig 4 Graph

IV. Results and Discussion

The deployment of the AI Fraud Detection system produced valuable results about how machine learning techniques stop financial crimes through transactions. Evaluation results showed that chosen algorithms performed well in prediction tasks due to their high level of accuracy. The Random Forest and Gradient Boosting algorithms proved most effective by reaching accuracy levels higher than 95% along with satisfactory precision and recall outcomes. Such model performance demonstrates how well the models recognize genuine from fraudulent transactions while generating few false positives to ensure user trust and workflow optimization.

Two ensemble models namely Random Forest and Gradient Boosting delivered the best outcomes because these systems demonstrate strong protection against overfitting while developing comprehensive data relationships. Data analysis showed that transaction amount together with user behavior patterns and transaction frequency respectively stood as the most predictive features for detecting fraud according to industry standards. Research on fraud indicators has become essential because it directs productive data collection methods toward fundamental indicators.

The system's real-time prediction system underwent different testing scenarios which verified its capability to process incoming transactions with speed below two seconds. A rapid response time remains essential because operational settings require prompt actions to stop fraud from occurring. The application encountered difficulties when trying to scale the model along with adapting to changes in fraudulent patterns. The obstacles we found together with possible data biases and model retraining needs demonstrate that operational fraud detection systems need continuous evaluation and maintenance.

The future research will concentrate on developing progressive abilities for the model to handle emerging fraud methods using progressive learning algorithms and incorporating auxiliary information including social media activity records and third-party database information. Expanding the use of deep learning techniques and additional machine learning approaches would reveal more advanced patterns that traditional systems overlook during analysis. The project shows how AI technology can successfully prevent financial crime while exposing potential development spaces for the evolving threats in the financial crime sector.

V. Conclusion

The AI Fraud Detection system created during this project has established a revolutionary step toward combating financial fraud. Machine learning enables this system to detect and forecast fraudulent transactions accurately which gives organizations a defensive security approach and financial loss reduction capability. The system operates with efficiency and responsiveness in real-time through the combination of data collection followed by preprocessing and feature engineering and model training evaluation and real-time prediction.

Random Forest along with Gradient Boosting demonstrated superior performance in detecting fraudulent behavior since they could examine several features at once for detecting fraudulent patterns. The discovery of vital features that affect fraud detection both enhances model execution and helps optimize data gathering approaches as well as system development.

This technique presents encouraging operational abilities alongside critical constraints which stress the necessity to systematically watch and alter it constantly. The system demands constant model maintenance through proactive measures because data problems and frequent fraud technique changes necessitate CMS to preserve its usefulness.

The present project creates basic infrastructure which will help future developers enhance the AI Fraud Detection field. Inserting advanced machine learning techniques together with expanded data sources would result in increased optimization of the system to face upcoming challenges. The investigation works toward developing sophisticated fraud detection technology which provides effective protection for digital financial operations.

VI. REFERENCES

[1] Ahmed, M., Hu, J., & Yao, X. (2016). "Anomaly detection in fraud detection using autoencoders." Journal of Computer Science and Technology, 31(1), 1-10.

[2] Chandola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly detection: A survey." ACM Computing Surveys, 41(3), 1-58.

[3] Ghosh, A., & Reilly, D. (1994). "Credit card fraud detection with a neural network." Proceedings of the IEEE International Conference on Neural Networks, 2, 155-159.

[4] Kumar, V., Singh, P., & Arora, A. (2021). "Real-time fraud detection using streaming data." Journal of Real-Time Computing, 2(1), 45-55.

[5] Li, C., Zhang, Y., & Zhao, Z. (2017). "Deep learning for fraud detection: An overview." Journal of Financial Data Science, 3(4), 65-78.

[6] Jouili, A., & Zohra, T. (2021). "Feature selection techniques for fraud detection." International Journal of Computer Applications, 98(5), 24-30.

[7] Hodge, V. J., & Austin, J. (2004). "A survey of outlier detection methodologies." Artificial Intelligence Review, 22(2), 85-126.

[8] Ruff, L., & Kloft, M. (2018). "Deep semi-supervised learning for fraud detection." Proceedings of the International Conference on Data Mining, 210-215.

[9] Sudhakar, K., & Gupta, J. N. (2019). Data Analytics on Consumer Behavior in Credit Card Industry. Journal of Emerging Technologies and Innovative Research, 6(3), 334–338.

[10] Balamurugan, A., GIriranjan, B., Sudhakar, K., Potluri, P., Kumar, K. R., & Sane, A. R. (2022). Data Management and Visual Information Processing in Financial Organisation using Machine Learning. 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS).

[11] Sudhakar, K., Sree, S. C., Meghana, L., Bhavana, S., & Durga, B. N. (2022). Identification of types of intrusion attacks using spark and gradient boosted tree classifier. International Journal For Innovative Engineering and Management Research, 11(4), 49–55.

[12] Sudhakar, K., & VSRK, P. G. (2015). Hadoop- a modern data architecture for accelerating earnings growth in banking and insurance. International Journal of Engineering Research-Online, 3(4), 415–419.

[13] Sudhakar, K., N, A., Biradar, S., Indira, B., Basha, S. S., & T, K. (2021). Empirical View Of Financial Management Survey In Block Chain Technology Issues, Risk And Mitigation. International Journal of Aquatic Science-IJAS, 12(1), 259–267.

[14] Mahalakshmi, N. V., Tejaswini, G., & Sudhakar, K. (2020). Feature Selection, based on teaching and learning based Optimization Algorithm. International Journal of Computer Science & Mechatronics-IJCSM, 1(1), 1–8.

[15] Sudhakar, K., Lavanya Valli, P., Charitha, V., Sasi Durga, G., & Sri Sai Leela, P. (2021). Data Poison detection schemes for Distributed Machine Learning. Mukt Shabd Journal, 10(7), 572–577.

[16] JSV, G. K., Rao, M. V., & Sudhakar, K. (2020). Various Algorithms & Techniques Driving Data Science for Big Data. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(5), 725–727.
[17] Kumar, H. P. A., Gokul, J. S., & Sudhakar, K. N. (2023). Intelligent Filter for Internet Traffic Monitoring and Analysis of Possible Cyber Threats. International Conference on ICT for Sustainable Development, 107–119.
[18] Sudhakar, K., Harsha, Siddika, K., Mallika, K. S., & Bharadhwaja, V. (2022). Synthetic media Deepfake Video Detection using ResNeXt & LSTM. International Journal For Innovative Engineering and Management Research, 11(6), 1471–1483.
[19] Zhang, Y., & Wu, X. (2021). "Feature selection and its applications in fraud detection: A review." ACM Computing Surveys, 54(3), Article 59.
[20] Yang, Y., & Wang, L. (2020). "Real-time fraud detection in financial transactions: A systematic review." Journal of Financial Crime, 27(3), 774-795.
[21] Mendez, J. S., & Ruiz, L. (2019). "Machine learning techniques for fraud detection: A comprehensive survey." IEEE Transactions on Neural Networks and Learning Systems, 30(6), 1734-1750.
[22] Balcázar, J. L., & Pina, A. A. (2021). "An overview of machine learning in fraud detection." Journal of Intelligent Systems, 30(1), 45-59.
[23] Chandrashekar, G., & Sahin, F. (2014). "A survey on feature selection methods." Computational Intelligence and Neuroscience, Article ID 198152.
[24] Kotsiantis, S. B., & Pintelas, P. E. (2004). "Predicting students' performance in distance learning using machine learning techniques." International Journal of Engineering Education, 20(3), 317-325.
[25] Zhang, Y., & Wang, T. (2018). "A survey on fraud detection in e-commerce: Models and methods." IEEE Access, 6, 490-504.
[26] Ruff, L., Vandermeulen, R., & Kloft, M. (2020). "Unsupervised anomaly detection with generative adversarial networks." Journal of Machine Learning Research, 21(110), 1-28.
[27] Kumar, V., & Singh, J. (2019). "Applications of machine learning in fraud detection: A survey." International Journal of Computer Applications, 178(24), 23-28.
[28] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
[29] Provost, F., & Fawcett, T. (2013). "Data science for business: What you need to know about data mining and data-analytic thinking." O'Reilly Media.
[30] Han, J., Kamber, M., & Pei, J. (2011). Data mining: Concepts and techniques. Elsevier.
[31] 1. Balcázar, J. L., & Pina, A. A. (2021). "An Overview of Machine Learning in Fraud Detection." Journal of Intelligent Systems, 30(1), 45-59. DOI: 10.1515/jisys-2020-0021.
[32] 2. Chandrashekar, G., & Sahin, F. (2014). "A Survey on Feature Selection Methods." Computational Intelligence and Neuroscience, 2014, Article ID 198152. DOI: 10.1155/2014/198152.
[33] 3. Kotsiantis, S. B., & Pintelas, P. E. (2004). "Predicting Students' Performance in Distance Learning using Machine Learning Techniques." International Journal of Engineering Education, 20(3), 317-325.
[34] 4. Zhang, Y., & Wang, T. (2018). "A Survey on Fraud Detection in E-commerce: Models and Methods." IEEE Access, 6, 490-504. DOI: 10.1109/ACCESS.2018.2799401.
[35] 5. Hodge, V. J., & Austin, J. (2004). "A Survey of Outlier Detection Methodologies." Artificial Intelligence Review, 22(2), 85-126. DOI: 10.1023/B