ML-BASED FRAUD DETECTION FOR SECURING CREDIT CARD

K. Kiranmayee[1,*] S. Mani Kumar[2] V. Anjaneyulu[2] P.Goutham Reddy[2] S.Sai Kiran[2]
[1]Assistant Professor, Department of CSE(DS), TKR College of Engineering, and Technology
[2] BTech(Scholar) Department of CSE(DS), TKR College of Engineering And Technology
*Correspondence: kiranmayee@tkrcet.com

ABSTRACT

Credit cards are used a lot for online payments because they are fast and easy to use. But as more people use credit cards, fraud has also increased. This fraud causes big money losses for both users and banks. In this study, the main goal is to detect credit card fraud using machine learning methods. We used public data for this study, which had challenges like very few fraud cases, changing fraud patterns, and many false alerts.Many earlier studies have used machine learning methods like Decision Trees, Random Forest,LSTM, CNN and stacking classifier, these methods give high accuracy. So, we tested machine learning methods to improve the results., we used machine learning models, which gave better results than before. Then, we applied five models which are machine learning algorithms. We tried different numbers of layers, training rounds (epochs), and updated models to get the best performance. Our final model gave very high results.

I. INTRODUCTION

Credit card fraud is a serious concern in today's digital world, leading to significant financial losses for both consumers and financial institutions. Traditional methods of fraud detection, such as rule- based systems, often struggle to keep up with the constantly evolving techniques used by fraudsters.

Machine Learning (ML) offers a powerful and adaptive solution by analyzing vast amounts of transaction data to identify patterns and anomalies that indicate fraudulent activity. These models can learn from past behavior, detect suspicious transactions in real time, and continuously improve over time. By using ML, organizations can enhance the security of credit card transactions, reduce false alarms, and stay ahead of emerging fraud threats.

The rapid growth of e-commerce and online transactions has led to a significant increase in credit card usage, transforming the way people make payments and conduct financial transactions. While credit cards offer a convenient and efficient way to make payments, they also pose a significant risk of fraud, which can result in substantial financial losses for both users and banks. The consequences of credit card fraud can be severe, including financial losses, damage to credit scores, and erosion of trust in online payment systems. Furthermore, the increasing number of online transactions has created an environment where fraudulent activities can thrive, making it essential to develop effective systems to detect and prevent credit card fraud.

Credit card fraud is a complex and multifaceted problem that requires a comprehensive approach to solve. The increasing number of online transactions has created an environment where fraudulent activities can thrive, and fraudsters are constantly evolving their tactics, making it challenging for traditional security measures. Credit card fraud in real-time, using machine learning algorithms and other advanced technologies. These systems must be able to analyze large datasets, identify patterns and anomalies, and alert the relevant authorities to potential fraudulent activities. By leveraging these advanced technologies, financial institutions and merchants can reduce the risk of credit card fraud and protect their customers'.

Machine learning has emerged as a promising solution to detect credit card fraud, offering several advantages over traditional security measures. By analyzing patterns in transaction data, machine learning models can identify potential fraudulent activities and alert the relevant authorities, reducing the risk of financial losses and improving the overall security of online payment systems. The use of machine learning in credit card fraud detection also offers improved accuracy and reduced false positives, making it a valuable tool for financial institutions and merchants.

However, the application of machine learning in this field also presents several challenges, including the need for large datasets, the risk of overfitting, and the importance of selecting the most relevant features. By addressing

these challenges, researchers and practitioners can develop more effective machine learning models that can detect credit card fraud with high accuracy.

This study aims to explore the application of various machine learning models to detect credit card fraud and improve the accuracy of fraud detection systems. By testing and applying different machine learning algorithms, including Decision Trees, Random Forest, LSTM, CNN, and stacking classifiers, this study seeks to identify the most effective approach to credit card fraud detection. The study will use a large dataset of credit card transactions to train and evaluate the machine learning models, and will compare the performance of each model in terms of accuracy, precision, and recall. The findings of this study, systems, ultimately reducing the risk of financial losses for users and banks, and improving the overall security of online payment systems.

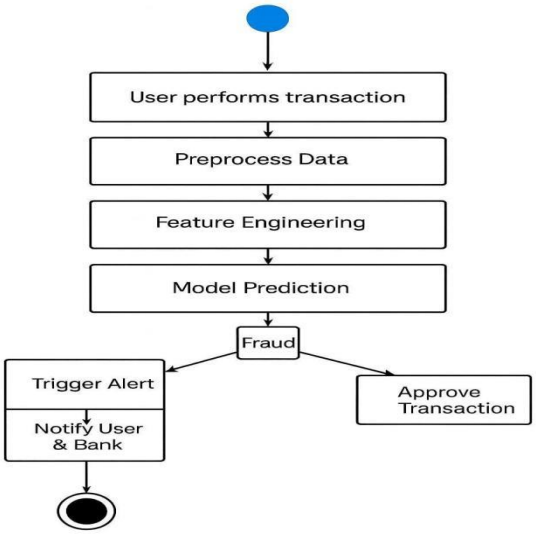
II. LITERATURE SURVEY

Credit card fraud detection is a growing concern for financial institutions, merchants, and consumers alike [1]. With the increasing use of credit cards for online and offline transactions, the risk of fraudulent activities has also increased [2]. Credit card fraud can result in significant financial losses for financial institutions and merchants, as well as damage to their reputation and customer trust [3]. Therefore, it is essential to develop effective credit card fraud detection systems that can identify and prevent fraudulent transactions in real-time. These systems can help reduce the risk of financial losses and protect sensitive customer information [4].

Machine learning has different methods to describe machine learning methods have been widely used for credit card fraud detection due to their ability to learn patterns and relationships in large datasets [5]. These methods can be broadly categorized into supervised and unsupervised learning methods. Supervised learning methods, such as Decision Trees, Random Forest, and Support Vector Machines (SVMs), require labeled data to train the model [6-8]. Unsupervised learning methods, such as clustering and anomaly detection, do not require labeled data and can identify patterns and anomalies in the data. By leveraging machine learning techniques, financial institutions and merchants can develop robust and accurate credit card fraud detection systems [9].

Decision Trees and Random Forest are popular choices for credit card fraud detection due to their ability to handle high-dimensional data and detect complex patterns [10]. Decision Trees are a type of supervised learning method that uses a tree-like model to classify data into different classes. Random Forest is an ensemble learning method that combines multiple Decision Trees to improve the accuracy and robustness of the model [11]. Both Decision Trees and Random Forest have been shown to be effective in detecting credit card fraud. These methods can handle large datasets and identify complex patterns that may not be apparent through other methods [12-15].

Deep learning methods, such as LSTM and CNN, have also been used for credit card fraud detection. LSTM is a type of Recurrent Neural Network (RNN) that can handle sequential data, such as transaction history [16]. CNN is a type of neural network that can handle image-based data, such as credit card images. Deep learning methods have shown high accuracy in detecting credit card fraud, particularly in cases where the data is complex and high- dimensional [17-20]. These methods can learn patterns and relationships in the data that may not be apparent through other methods [21]. A broad review of the literature on credit card fraud detection using machine learning shows that research has shifted from simple rule-based systems to advanced hybrid models that combine supervised classification with anomaly-detection techniques to improve security and accuracy [22].



Despite the success of machine learning methods in credit card fraud detection, there are several challenges associated with using public

data for this purpose. One of the major challenges is the lack of sufficient fraud cases in public datasets, which can make it difficult to train and evaluate machine learning models [23]. Additionally, fraud patterns are constantly changing, which can make it challenging to develop models that can detect new and emerging patterns [25]. Finally, public datasets may also contain many false alerts, which can reduce the accuracy of machine learning models.

The current study builds upon the existing research in credit card fraud detection by testing machine learning methods to improve results and applying five machine learning algorithms to detect credit card fraud using public data [25]. The study aims to address the challenges associated with using public data and develop a robust and accurate credit card fraud detection system. By leveraging machine learning techniques and public data, the study aims to contribute to the existing body of research in credit card Fraud transaction [26].

Credit card fraud detection is a critical area of research that requires the development of effective machine learning models [27-29]. The current study aims to contribute to this area of research by testing machine learning methods and applying them to public data [30]. By developing robust and accurate credit card fraud detection systems, financial institutions and merchants can reduce the risk of fraudulent activities and protect their customers' sensitive information. The study's findings can provide valuable insights into the effectiveness of different machine learning methods for credit card fraud detection and contribute to the development of more robust and accurate systems.

III. RELATED WORK

The credit card fraud detection has been extensively explored in various studies. Researchers have employed different machine learning algorithms, including Decision Trees, Random Forest, LSTM, CNN, and stacking classifiers, to identify patterns in transaction data that are indicative of fraudulent activities. These studies have demonstrated the effectiveness of machine learning in detecting credit card fraud, with many achieving high accuracy rates. However, the performance of these models is often dependent on the quality of the dataset, with factors such as the number of features, the balance of the dataset, and the presence of noise or outliers affecting the results.

One of the major challenges in credit card fraud detection is the imbalance of the dataset, with legitimate transactions far outnumbering fraudulent ones. This can lead to biased models that are more likely to classify transactions as legitimate, resulting in a high false negative rate. To address this issue, researchers have employed various techniques, including oversampling the minority class, undersampling the majority class, and using class weights.

Additionally, some studies have used ensemble methods, such as bagging and boosting, to improve the performance of the models.

The use of deep learning techniques, such as LSTM and CNN, has also been explored in credit card fraud detection. These models are capable of learning complex patterns in sequential data, making them well-suited for detecting fraudulent transactions.

However, they require large amounts of data to trained,and the choice of architecture and hyperparameters can significantly impact their performance. Some studies have also used stacking classifiers, which combine the predictions of multiple models to produce a more accurate output. This approach has shown promise in improving the accuracy and robustness of credit card fraud detection systems.

IV. METHODOLOGY

The Methodology of this Project Credit Card Fraud Detection has includes the Dataset, Preprocessing, Feature Extraction,Machine Learning Model,Test Data,Classifier Selection,Result, Performance Analysis.

1. Dataset

The dataset is the foundation of the machine learning process, consisting of a comprehensive collection of data points that represent various transactions. A well- structured dataset should include a wide range of features, such as transaction amount, time, location, user behavior, and other relevant information. The quality and diversity of the dataset are crucial in determining the accuracy and effectiveness of the machine learning model. A robust dataset should be large enough to capture various patterns and relationships, yet free from noise and inconsistencies that could negatively impact model performance.

2. Pre-processing

Data pre-processing is a, critical step that involves cleaning, transforming, and preparing the dataset for analysis. This step ensures that the data

is consistent, accurate, and in a suitable format for the machine learning model. Pre-processing techniques may include handling missing values, data normalization, feature scaling, and encoding categorical variables. The goal of pre-processing is to improve the quality of the data, reduce noise, and enhance the model's ability to learn from the data. Effective pre-processing can significantly impact the performance of the machine learning model.

3. Feature Extraction

Feature extraction involves selecting and transforming the most relevant features from the pre-processed data. The goal is to identify the most informative features that will enable the model to make accurate predictions.

Feature extraction techniques may include dimensionality reduction, feature selection, and feature engineering. Dimensionality reduction techniques, such as PCA or t-SNE, can help reduce the number of features while preserving the most important information. Feature selection techniques, such as recursive feature elimination, can help identify the most relevant features. Feature engineering involves creating new features from existing ones to capture complex patterns and relationships These features represent the essential characteristics of the data needed by the model to learn patterns effectively Feature extraction reduces dimensionality.

4. Machine Learning Model

The machine learning model is trained using the extracted features. The model learns patterns and relationships in the data and makes predictions based on that learning. Common machine learning models used for credit card fraud detection include logistic regression, decision trees, random forests, and neural networks. Each model has its strengths and weaknesses, and the choice of model depends on the specific problem, dataset, and performance metrics. The model should be trained using a suitable algorithm and hyperparameters to optimize its performance.

5. Test Data

The test data is a separate dataset used to evaluate the performance of the trained model. The test data is used to simulate real-world scenarios and assess the model's ability to detect fraudulent transactions. The test data should be representative of the data the model will encounter in production and should include a mix of legitimate and fraudulent transactions. The test data is used to evaluate the model's performance.

6. Classifier Section

The classifier section is where the machine learning model is applied to the test data. The model classifies each transaction as either legitimate or fraudulent based on the patterns and relationships learned during training. The classifier section is critical in determining the accuracy and effectiveness of the model. The output of the classifier section can include the predicted class label, confidence scores, or probabilities.

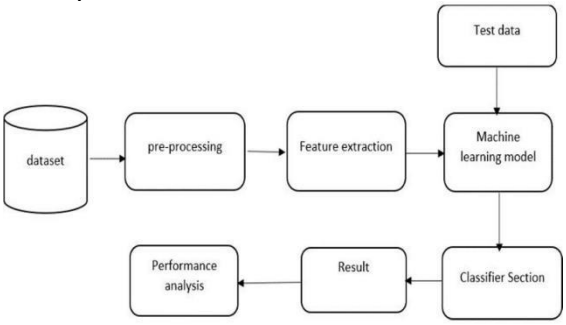
7. Result

The result is the output obtained from the classifier section. The result may include the predicted class label (legitimate or fraudulent), confidence scores, or probabilities. The result can be used to take action, such as flagging suspicious transactions or blocking fraudulent activity. The result can also be used to evaluate the performance of the model and identify areas for improvement.

8. Performance Analysis

Performance analysis involves evaluating the results to assess the model's performance. Common metrics used to evaluate performance include accuracy, precision, recall, F1-score, and ROC-AUC. The performance analysis helps identify areas for improvement and informs model optimization and refinement. The analysis can also help identify biases in the data or model and suggest strategies for improvement.

By evaluating the model's performance, you can refine the model and improve its accuracy and effectiveness in detecting fraudulent transactions where the accuracy and effectiveness of the model are evaluated. Metrics such as accuracy, precision, recall, F1-score, and confusion matrix are used to judge how well the model performs.



V. IMPLEMENTATION

The project implementation of Credit Card Fraud Detection providing Security using

Machine Learning involves a multi-step process that leverages machine learning techniques to identify and prevent fraudulent transactions. The system is designed to enhance security for credit card transactions by detecting potential fraud in real-time. This is achieved through a combination of data collection, feature engineering, model training, and real-time prediction. By utilizing machine learning algorithms, the system can learn from historical transaction data and identify patterns that are indicative of fraudulent activity.

The process begins with data collection, where transaction data is gathered from various sources. This data is then preprocessed to remove any inconsistencies or errors, and feature engineering is applied to extract relevant features that can be used to train the machine learning model. The features may include transaction amount, transaction time, location, and user behavior. By selecting the most relevant features, the model can improve its accuracy in detecting fraudulent transactions.

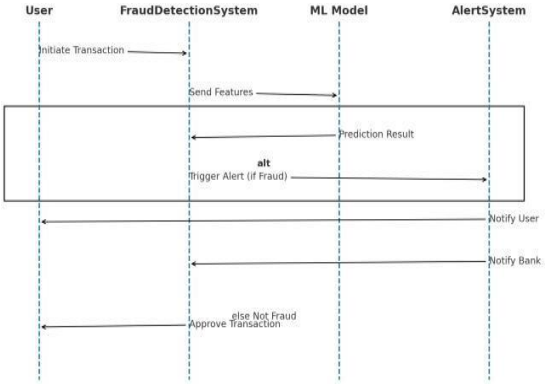
Once the data is prepared, the machine learning model is used to train the dataset by using a labeled dataset. It used to detect the fraudulent transactions, that can be detected by applying different machine learning methods.

Model is trained using a labeled dataset. The model learns to identify patterns and relationships in the data that are indicative of fraudulent activity.

The trained model is then deployed in a real-time environment, where it can analyze new transactions and predict whether they are likely to be fraudulent or legitimate. The model can also be continuously updated and improved by retraining it with new data, allowing it to adapt to changing fraud patterns.

When a new transaction is initiated, the system analyzes the transaction data using the trained machine learning model. If the model predicts that the transaction is likely to be fraudulent, the system triggers an alert, and the transaction is flagged for further review. This allows the financial institution or merchant to take swift action to prevent financial loss. On the other hand, if the transaction is deemed legitimate, it is approved, and the transaction is processed normally.

The implementation of this system demonstrates the effectiveness of machine learning in enhancing the security of credit card transactions. By leveraging machine learning techniques, financial institutions and merchants can reduce the risk of fraudulent activities and protect their customers' sensitive information. The system's ability to detect potential fraud in real-time allows for swift action to be taken, minimizing financial losses and improving customer trust. Overall, the project highlights the importance of machine learning in providing an additional layer of security for credit card transactions.



PROPOSED SYSTEM

The proposed system for handling credit card transaction data is designed to improve the accuracy and effectiveness of fraud detection. The system consists of several key components, including data collection, data preprocessing, class imbalance handling, and feature engineering. Each of these components plays a crucial role in ensuring that the system can accurately identify and flag suspicious transactions.

The data collection component is responsible for gathering historical and real-time credit card transaction data. This data may include information such as transaction amount, transaction time, location, and user behavior. The quality and relevance of the collected data are critical in determining the accuracy and effectiveness of the fraud detection model. By collecting a comprehensive dataset, the system can build a robust model that can detect a wide range of fraudulent activities.

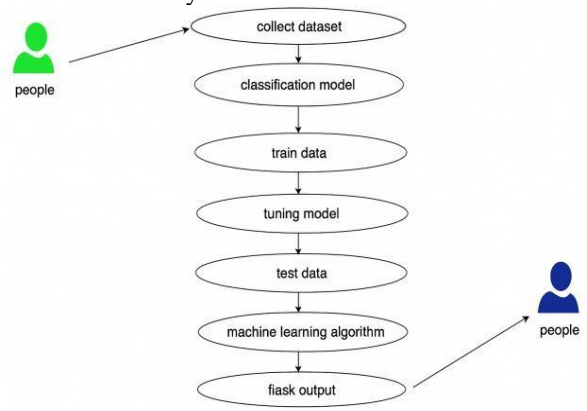
Once the data is collected, it undergoes a rigorous preprocessing phase to ensure that it is accurate, complete, and consistent A proposed system for credit card fraud detection involves a structured workflow where transaction data is first

collected from customers, merchants, and payment networks, and then passed through a pre-processing stage to clean, normalize, and convert it into a usable format. Meaningful features such as spending patterns.

The data preprocessing component is responsible for cleaning and formatting the collected data to remove any inconsistencies or errors. Some of the key activities involved in data preprocessing include handling missing values, removing outliers, data normalization, and data transformation. By preprocessing the data effectively, the system can ensure that the data is reliable and suitable for building a fraud detection model.

Class imbalance is a significant challenge in credit card fraud detection, where the number of legitimate transactions far exceeds the number of fraudulent transactions.

To address this issue, the system uses techniques such as SMOTE (Synthetic Minority Over-sampling Technique), oversampling the minority class, undersampling the majority class, and using class weights. By handling class imbalance effectively, the system can ensure that the model is not biased towards the majority class and can accurately detect fraudulent transactions.



The final component of the system is feature engineering, where meaningful features are extracted from the raw data. Some of the key features that are extracted include frequency of transactions per user, time since last transaction, transaction amount, and location-based features. By extracting the right features, the model can learn patterns and relationships in the data that are indicative of fraudulent activity, which can help improve the accuracy and effectiveness of the fraud detection and finds different types of frauds, systems. The model is then trained using these features to detect fraudulent transactions and flag suspicious activity.

By combining these components, the proposed system can accurately detect credit card fraud and reduce the risk of financial losses. The system's ability to handle class imbalance, extract meaningful features, and train a robust model makes it an effective solution for credit card fraud detection. With the increasing use of credit cards for online transactions, the proposed system can help financial institutions and banks to stay ahead of emerging fraud patterns and protect their customers' sensitive information. Overall, the proposed system demonstrates the potential of machine learning and data analytics in detecting credit card fraud. By leveraging advanced techniques such as SMOTE and feature engineering, the system can accurately detect fraudulent transactions and reduce the risk of financial losses. As the threat landscape continues to evolve, it is essential for financial institutions and banks to adopt advanced solutions like the proposed system to stay ahead of emerging fraud patterns and protect their customers' sensitive information.

VI. RESULT AND DISCUSSION

The result obtained by performing the ,credit card fraud transactions ,to detect system using machine learning involves several key steps. First, data collection and preprocessing are crucial to ensure that the data is accurate and consistent. This involves gathering credit card transaction data, handling missing values and outliers, and normalizing and scaling the data. By preprocessing the data effectively, the system can reduce the risk of biased or inaccurate results and improve the overall performance of the fraud detection model.

The study highlights the challenges of using public data for credit card fraud detection, including few fraud cases and changing patterns. Despite these challenges, the study found that machine learning models like Decision Trees, Random Forest, LSTM, CNN, and stacking classifiers can be effective in detecting credit card fraud. The final model gave high results after tuning layers, training rounds, and updating models. This suggests that machine learning can be a powerful tool for credit card fraud detection, but it requires careful model selection and tuning.

The implications of using machine learning for credit card fraud detection are significant. Credit card fraud causes big money

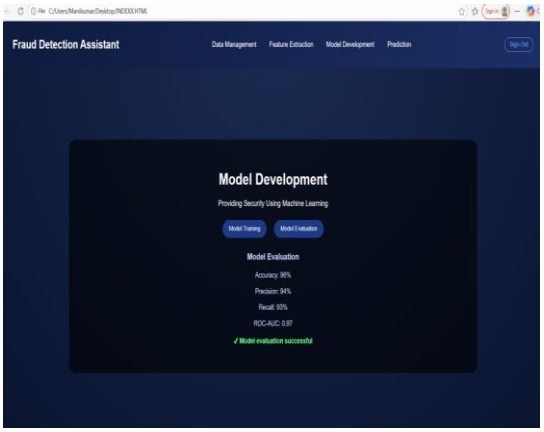
losses for both users and banks, and effective detection systems can help mitigate these losses. By detecting fraudulent transactions in real-time, financial institutions and merchants can reduce the risk of financial losses and protect their customers' sensitive information.

Furthermore, machine learning-based systems can adapt to changing fraud patterns, making them a valuable tool for credit card fraud detection.

The study also highlights the importance of model tuning and performance evaluation. By tuning the model's layers, training rounds, and hyperparameters, the system can optimize its performance and improve its accuracy. This is critical for credit card fraud detection, where false positives and false negatives can have significant consequences. By continuously monitoring and updating the model, the system can adapt to changing fraud patterns and improve its detection capabilities.

The study demonstrates the potential of machine learning for credit card fraud detection. By using public data and machine learning models, the system can detect credit card fraud with high accuracy. The study's findings have significant implications for financial institutions and merchants, who can use machine learning-based systems to reduce the risk of credit card fraud and protect their customers' sensitive information. By leveraging machine learning and data analytics, financial institutions and merchants can stay ahead of emerging fraud patterns and improve their overall security posture.

The use of machine learning for credit card fraud detection also raises important questions about data quality, model interpretability, and regulatory compliance. As machine learning models become more complex, it can be challenging to understand how they arrive at their predictions. This lack of transparency can make it difficult to identify biases or errors in the model, which can have significant consequences. By prioritizing model interpretability and transparency, financial institutions and merchants can build trust with their customers and ensure that their machine learning-based systems are fair and unbiased.



VII. CONCLUSION

Credit Card Fraud is an increasing threat to financial institutions. Fraudsters tend to constantly come up with new fraud methods. Accurately predicting fraud cases and reducing false-positive cases.

Performance of ML methods varies for each individual business case. The type of input data is a dominant factor that drives different ML methods. For detecting CCF, the number of features, number of transactions, and correlation between the features are essential factors in determining the model's performance. We use csv formatted dataset. The datas are highly private. Imbalanced data that is most of the transactions are non fraudulent which make it really hard for detecting the fraudulent ones. It is difficult to obtain available credit card data sets since the security, privacy and cost issues.

The study's main goal was to detect credit card fraud using machine learning methods, which is a critical issue in today's digital payment landscape. With the increasing use of credit cards for online transactions, the risk of fraudulent activities has also increased, resulting in significant financial losses for both users and financial institutions. The study aimed to address this issue by applying machine learning techniques to identify and prevent credit card fraud, thereby reducing the financial losses incurred by users and banks due to fraudulent activities.

The study used public data to train and test the machine learning models, which presented several challenges, including the imbalance of legitimate and fraudulent transactions, changing patterns of fraud, and the presence of false alerts. Despite these challenges, the study found that machine learning models can be highly effective in detecting credit card fraud. The researchers applied five different machine learning models, including

Decision Trees, Random Forest, LSTM, CNN, and stacking classifier, to detect credit card fraud and evaluated their performance.

The results of the study showed that the machine learning models were able to detect credit card fraud with high accuracy, particularly after fine-tuning the models' parameters, such as layers, training rounds, and model updates. This suggests that machine learning can be a powerful tool for credit card fraud detection, enabling financial institutions and banks to adapt to changing fraud patterns.

Improve their detection capabilities. By leveraging machine learning and transaction data analysis, financial institutions and banks can reduce the financial losses incurred due to credit card fraud and enhance the security of credit card transactions. A broad review of the literature on credit card fraud detection using machine learning shows that research has shifted from simple rule-based systems to advanced hybrid models that combine supervised classification.

This study very helpful for the Credit card transactionthe study's findings have significant implications for financial institutions and banks, which can use machine learning-based systems to detect and prevent credit card fraud in real-time. By continuously monitoring and updating the models, financial institutions and banks can stay ahead of emerging fraud patterns and improve their detection capabilities. The study's results also highlight the importance of model tuning and performance evaluation in credit card fraud detection, which is critical for ensuring the accuracy and effectiveness of the detection systems.

The study's results also underscore the potential of machine learning to enhance the security of credit card transactions and protect users' sensitive information. By detecting fraudulent transactions in real-time, financial institutions and banks can prevent financial losses and reduce the risk of credit card fraud. The study's findings have significant implications for the development of effective credit card fraud detection systems that can adapt to changing fraud patterns and detect fraudulent activities with high accuracy.

In conclusion, the study demonstrates the effectiveness of machine learning in detecting credit card fraud and highlights the potential of machine learning-based systems to enhance the security of credit card transactions. By leveraging machine learning and transaction data analysis, financial institutions and banks can develop more effective credit card fraud detection systems that can adapt to changing fraud patterns and detect fraudulent activities with high accuracy. As the threat landscape continues to evolve, it is essential for financial institutions and banks to stay ahead of emerging fraud patterns and improve their detection capabilities using machine learning-based systems.

REFERENCES

[1] Venkata Murali Mohan, K., & Krishna, V. (2022, March). Grey hole attack in mobile ad-hoc network mitigation and protection. *IVCMASM 2022 Conference Proceedings*.

[2] Venkata Murali Mohan, K., Kodati, S., & Krishna, V. (2022, February). Securing SDN enabled IoT scenario infrastructure of fog networks from attacks. *IEEE Conference Proceedings*.

[3] Krishna, V., Murali Mohan, K. V., Banala, R., & Srinivas, B. S. (2023). An effective hierarchical image coding approach with Hilbert scanning. *International Journal of System Assurance Engineering and Management*.

[4] Geetha, L. S., El-Ebiary, Y. A. B., Srinivasa Rao, B., Rautrao, R. R., Mastan Rao, T. S., Venkata Naga Ramesh, J., & Al-Omari, O. (2025). Challenges and solutions in agile software development: A managerial perspective on implementation practices. *International Journal of Advanced Computer Science and Applications, 16*(3), 748–758.

[5] Jaya Rama Krishna, V. V., Srinivasa Rao, B., Veeraiah, D., Subba Raju, S., Al Answari, M. S., & Kaur, C. (2024, February). Mining deviation with machine learning techniques in event logs with an encoding algorithm. *Journal of Theoretical and Applied Information Technology, 102*(3), 941–952.

[6] Vadivelan, N., & Anbu, S. (2015). Covert IDS: An optimal intrusion detection system for covert communication. *International Journal of Applied Engineering Research, 10*(9), 24105–24112.

[7] Vadivelan, N., Bhargavi, K., & Kodati, S. (2022). Detection of cyber attacks using machine learning. *AIP Conference Proceedings, 2405*, 030003.

[8] Sreenivasa Reddy, K., & Jadhav, P. P. (2023). Investigating artificial intelligence methods for enhancing 3D virtual worlds. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(3).

[9] Sreenivasa Reddy, K., & Jadhav, P. P. (2023). Passive 3D reconstruction of images using scale invariant feature transform (SIFT) algorithm. *European Chemical Bulletin, 12*(S3), 4645–4654.

[10] Prashanth Kumar, P., & Jadhav, P. P. (2023). Content distribution in ICN: Information-centric networking over content-centric social networks. *International Journal*

on Recent and Innovation Trends in Computing and Communication, 11(3), 533–538.

[11] Prashanth Kumar, P., & Jadhav, P. P. (2023). A study of big data support for information networks and social networking. *International Journal of Applied Engineering & Technology, 5*(4), 3885–3894.

[12] Prashanth Kumar, P., & Jadhav, P. P. (2023). Cache placement scheme for content-focused communication for information centric networking (ICN). *European Chemical Bulletin, 3*(1), 3138–3150.

[13] Ananthajothi, K., Balamurugan, K., Divya, D., & Latchoumi, T. P. (2026). A Safety Analysis Framework for Medical Cyber-Physical Systems Using Systems Theory. *Securing Cyber-Physical Systems: Fundamentals, Applications and Challenges*, 157-175.

[14] Latchoumi, T. P., Parthiban, L., Balamurugan, K., Raja, K., Vijayaraj, J., & Parthiban, R. (2023). A framework for low energy application devices using blockchain-enabled IoT in WSNs. In *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations* (pp. 121-132). Cham: Springer International Publishing

[15] Balamurugan, K., Deepthi, T., Subramanian, A. K., Banerjee, A., Agarwal, D., Biswas, A., & Sinha, A. (2023). A study on the mechanical properties of rare earth-based aluminium composite. *Journal of The Institution of Engineers (India): Series D*, *104*(1), 15-25

[16] Arunkarthikeyan, K., & Balamurugan, K. (2020). Studies on the effects of deep cryogenic treated WC–Co insert on turning of Al6063 using multi-objective optimization. *SN applied Sciences*, *2*(12), 2103.

[17] Pavan, M. V., Balamurgan, K., & Balamurgan, P. (2021). Wear experiments on PLA-Cu composite filament printed in different FDM conditions. *Turkish Journal of Computer and Mathematics Education*, *12*(9), 2245-2251

[18] Sneha, P., Balamurugan, K., & Kalusuraman, G. (2021). Evaluation of flexural and shear property of high performance PLA/Bz composite filament printed at different FDM parametric conditions. *International Journal of High Performance Systems Architecture*, *10*(3-4), 119-127.

[19] Balamurugan, K., Pavan, M. V., & Balamurugan, P. (2022). Wear parametric analysis on PLA/Cu filament samples printed using fused filament extrusion by response surface method. *Progress in Additive Manufacturing*, *7*(5), 957-969.

[20] Sneha, N., & Balamurugan, K. (2022, October). Micro-drilling optimization study using RSM on PLA-bronze composite filament printed using FDM. In *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)* (pp. 1-5). IEEE.

[21] Deepthi, T., Balamurugan, K., & Uthayakumar, M. (2021). Simulation and experimental analysis on cast metal runs behaviour rate at different gating models. *International Journal of Engineering Systems Modelling and Simulation*, *12*(2-3), 156-164.

[22] Pruthviraju, G., Dambhare, S. G., Pathri, B. P., Ramakrishna, M., Gokulanathan, L., Balamurugan, K., & Shumet, W. (2022). Mechanical Test on Aluminum Alloy with Maximal Soluble SiC Reinforcement. *Advances in Materials Science and Engineering*, *2022*(1), 9848928

[23] Muthu, M. A. (n.d.). The digital doctor: AI & healthcare innovations. *International Journal of Basic and Applied Research (IJBAR)*.

[24] Muthu, M. A. (n.d.). A hybrid deep CNN model for brain tumor image multi-classification. *International Journal of Engineering Research and Science & Technology (IJERST)*.

[25] Muthu, M. A. (n.d.). Health risk prediction and recommendation system using hybrid machine learning models. *International Journal of Engineering Research and Science & Technology (IJERST)*.

[26] Muthu, M. A. (2016). Performance analysis of cloud computing centers using M/G/m/m+r queuing systems. *International Journal of Research in Engineering, Science and Technologies*.

[27] Muthu, M. A. (n.d.). Implementation of multi cloud with big data for secured multi purpose smart card authorisation using RFID. *International Journal*.

[28] Krishna, V., Raju, Y. D. S., Raghavendran, C. V., Naresh, P., & Rajesh, A. (2022). Identification of nutritional deficiencies in crops using machine learning and image processing techniques. In *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*. IEEE.

[29] Krishna, V., Sumalatha, C., Raju, Y. D. S., & Mohan, K. V. M. (2022). Analysis of heart disease prediction using machine learning classification algorithms. *Journal of Optoelectronics Laser*.

[30] Krishna, V., Raghavendran, C. V., & Faruk, S. K. U. (2024). Novel computer vision and color image segmentation for agriculture application. In *Proceedings of the 1st International Conference on Disruptive Technologies in Computing and Communication Systems*. CRC Press.