Real-Time Credit Card Fraud Detection Using Machine Learning with Interactive Web Dashboard

Bolla Geetha sri[1], Umamaheswararao Mogili[2], M. Lava Kumar[3], S. Raju[4], K. Lavanya[5], V. Lokesh[6], D. Charan Chandu[7], Chandaka Guna Sekhar[8]

[1,2,8]Assistant Professor, Department of Computer Science and Engineering, Avanthi's St Theressa Institute of Engineering and Technology, Garividi, Andhra Pradesh, India

[3,4,5,6,7] B.Tech, Department of Computer Science and Engineering, Avanthi's St Theressa Institute of Engineering and Technology, Garividi, Andhra Pradesh, India

doi.org/10.64643/IJIRTV12I11-195537-459

***Abstract*—The rapid growth of digital payment systems has significantly increased the risk of credit card fraud, leading to substantial financial losses for banks and customers. Detecting fraudulent transactions in real time is challenging due to the large volume of transactions and the highly imbalanced nature of fraud datasets. This study proposes a machine learning–based credit card fraud detection system integrated with an interactive web application for analyzing and visualizing fraud patterns. The system processes transaction datasets through stages including data preprocessing, feature selection, model training, and evaluation. Multiple machine learning algorithms such as Isolation Forest, Linear Support Vector Machine, and Logistic Regression are implemented to identify suspicious transactions and classify them as fraudulent or legitimate. The proposed framework also includes a web-based dashboard that allows users to upload datasets, execute detection models, and visualize fraud statistics and performance metrics. Experimental results demonstrate that machine learning techniques can effectively identify fraudulent activities while maintaining a balance between detection accuracy and false alarm rates. The system provides a scalable and user-friendly solution that can assist financial institutions in improving transaction monitoring and reducing fraud related risks.**

***Index Terms*—Credit Card Fraud Detection, Machine Learning, Isolation Forest, Support Vector Machine, Logistic Regression.**

I. INTRODUCTION

The rapid expansion of digital payment systems, online banking, and e-commerce platforms has significantly increased the use of credit cards for financial transactions. While these technologies have improved the convenience and speed of payments, they have also created opportunities for fraudulent activities. Credit card fraud has become one of the most critical challenges faced by financial institutions, resulting in substantial financial losses and reduced customer trust. As the volume of electronic transactions continues to grow, traditional fraud detection methods are becoming less effective in identifying sophisticated fraudulent behavior. Conventional fraud detection systems often rely on rule-based approaches, where predefined rules are used to identify suspicious transactions.

Although these systems provide basic protection, they struggle to detect new and evolving fraud patterns. Fraudsters constantly develop new techniques to bypass existing security mechanisms, making it difficult for static rule-based systems to detect complex fraud scenarios. Additionally, the highly imbalanced nature of transaction data, where fraudulent transactions represent only a small fraction of total transactions, further complicates the detection process. Machine learning techniques have emerged as powerful tools for addressing these challenges. By analyzing large volumes of transaction data, machine learning algorithms can automatically learn patterns associated with normal and fraudulent transactions. These models can identify hidden relationships within the data and adapt to changing fraud behaviors, making them more effective than traditional detection methods. As a result, machine learning-based fraud detection systems have gained significant attention in both academic research and financial industries. In this study, a machine learning-based credit card fraud detection system is proposed to identify fraudulent transactions efficiently.

The system utilizes algorithms such as Isolation Forest, Linear Support Vector Machine, and Logistic Regression to analyze transaction data and classify transactions as fraudulent or legitimate. In addition to the machine learning component, a web-based application is developed to allow users to upload transaction datasets, run fraud detection models, and visualize results through an interactive dashboard. The proposed system aims to provide an intelligent and scalable solution for fraud detection by combining data analysis, machine learning techniques, and web technologies. By improving the accuracy and efficiency of fraud detection, the system can help financial institutions enhance transaction security and minimize financial losses caused by fraudulent activities.

II. LITERATURE SURVEY

The rapid growth of electronic payment systems and online commerce has significantly increased the use of credit cards worldwide. While credit cards offer convenience and flexibility, they have also become a major target for fraudulent activities. Credit card fraud causes substantial financial losses to banks, merchants, and customers, making fraud detection a critical concern for financial institutions. Early fraud detection systems relied on traditional rule-based and manual verification techniques, which were ineffective in handling large volumes of transaction data and adapting to evolving fraud patterns. Some of the sample artificial intelligence, machine learning and deep learning models for prediction for fire detection are described in details [1-8]. Studies indicate that these conventional methods resulted in high false-positive rates and poor detection of new fraud behaviours, thereby reducing system efficiency and customer trust [9]. Research literature classifies credit card fraud into several categories, including lost or stolen card fraud, counterfeit card fraud, application fraud, mail-order and telephone-order fraud, and card-not-present fraud. Among these, card-not-present fraud has gained prominence due to the rapid expansion of e-commerce platforms. Delamaire et al. emphasized that fraud detection is a complex and cost-sensitive task, as incorrect classification of genuine transactions can lead to customer dissatisfaction and ethical concerns. This complexity motivated the adoption of intelligent and automated fraud detection systems capable of learning from historical transaction data [10]. With advancements in machine learning and data mining, fraud detection began to be modeled as a binary classification problem, where transactions are classified as either legitimate or fraudulent. Supervised learning techniques such as Logistic Regression, Support Vector Machines (SVM), Decision Trees, and Random Forests have been extensively explored in the literature. Logistic Regression, particularly with the sigmoid function, has been widely used as a baseline model due to its simplicity, interpretability, and ability to estimate the probability of fraudulent transactions. However, several studies report that Logistic Regression struggles to capture complex nonlinear fraud patterns present in real-world transaction data [11].

Support Vector Machines have been introduced to overcome some of these limitations by constructing optimal decision boundaries in high-dimensional feature spaces. Research shows that SVM can achieve higher classification performance than traditional statistical methods; however, its effectiveness is often limited by parameter sensitivity and severe class imbalance in credit card datasets. Many studies highlight that SVM performance degrades when fraudulent transactions represent only a small fraction of the data, which is a common characteristic of real-world fraud datasets [12]. Class imbalance is consistently identified as one of the most significant challenges in credit card fraud detection. Fraudulent transactions typically account for less than one percent of total transactions, causing standard classifiers to be biased toward predicting the majority class. As a result, accuracy alone is considered a misleading evaluation metric. Researchers strongly recommend using precision, recall, F1-score, and ROC-AUC to assess fraud detection performance. In particular, recall is emphasized as a critical metric because failing to detect fraudulent transactions leads directly to financial loss [13]. To address the limitations of supervised learning and the imbalance problem, researchers have explored unsupervised and anomaly detection approaches. Isolation Forest has emerged as an effective technique for identifying fraudulent transactions by isolating anomalous data points. Unlike supervised methods, Isolation Forest does not rely on labelled data and can detect rare fraud patterns by analyzing deviations from normal transaction behaviour. Studies demonstrate that Isolation Forest is computationally efficient, scalable, and capable of adapting to evolving fraud strategies, making it suitable for real-time fraud detection systems [14]. Recent literature highlights the importance of feature engineering in improving fraud detection accuracy. Rather than relying solely on raw transaction attributes such as amount and time, researchers propose extracting behavioural and aggregated features that capture spending patterns over time. Transaction aggregation and behavioural feature extraction significantly improve detection performance and reduce financial loss.

Temporal features, transaction frequency, and spending behaviour analysis have been shown to provide deeper insights into customer activity and help distinguish fraudulent behaviour from legitimate usage [15]. Fraud detection is also recognized as a cost-sensitive problem, where the consequences of false negatives and false positives differ significantly. Several studies propose cost-sensitive learning frameworks to balance financial loss and customer inconvenience. Additionally, real-time fraud detection has gained increasing attention, with researchers emphasizing the need for adaptive models capable of handling streaming transaction data and concept drift. Feedback mechanisms and periodic model updates are recommended to maintain detection performance as fraud patterns evolve over time [16]. Comprehensive survey studies provide a comparative analysis of various machine learning techniques used in credit card fraud detection. These studies highlight key challenges such as data privacy, scarcity of real-world datasets, interpretability of models, and adaptability to changing fraud behaviours. The findings suggest that no single algorithm can effectively address all fraud detection challenges. Instead, hybrid approaches that combine supervised and unsupervised learning techniques offer better robustness and reliability [17]. Secure Data Storage and Sharing in Multi-Cloud Environment In the cloud storage is also described to store the predicted data in a secured way [18-23].

III. METHODOLOGY

The proposed methodology analyzes credit card transaction data to identify fraudulent activities using machine learning techniques. The system processes transaction records and evaluates each transaction based on its statistical and behavioral attributes. The methodology involves extracting useful features from the dataset and applying classification and anomaly detection algorithms to distinguish fraudulent transactions from legitimate ones. The overall fraud detection process involves several stages including data preprocessing, feature extraction, model training, and prediction. Machine learning algorithms learn patterns from historical transaction data and use these patterns to classify new transactions. The computation of fraud detection involves the following steps:

1. Transaction Analysis: Evaluating the characteristics of each transaction such as transaction amount, time, and other relevant attributes.
2. Feature Extraction: Identifying important features that help distinguish fraudulent behavior from normal transaction patterns.
3. Model Training: Training machine learning models using labeled transaction data.
4. Fraud Prediction: Classifying new transactions as fraudulent or legitimate based on the trained models.

Unlike traditional rule-based fraud detection systems, the proposed approach utilizes machine learning models that can automatically learn complex patterns from transaction data. The system processes large datasets efficiently and improves fraud detection accuracy by analyzing historical transaction behavior.

3.1. Divide and Conquer Strategy

To handle large transaction datasets efficiently, a divide-and-conquer strategy is applied. The dataset is divided into smaller subsets, allowing faster data processing and improved model performance. Each subset of data is processed independently during preprocessing and training stages, and the results are combined to produce the final fraud detection outcome. The preprocessed dataset is then used to train machine learning models.

3.2. Feature Selection

Feature selection is used to identify the most relevant attributes from the transaction dataset that contribute to fraud detection. Important features such as transaction amount, time interval between transactions, and statistical transaction patterns are selected to improve model performance. These selected features are used as inputs for machine learning algorithms. Proper feature selection helps reduce model complexity and improves prediction accuracy.

3.3. Machine Learning Algorithms

Machine learning algorithms are used to classify transactions based on their characteristics. In this system, multiple models are used to detect fraudulent activities:

1. Isolation Forest: Used for anomaly detection to identify unusual transactions.
2. Linear Support Vector Machine (LinearSVC): Used for classification of fraudulent and legitimate transactions.
3. Logistic Regression: Used as a binary classification model to predict fraud probability.

These models analyze historical transaction data and learn patterns that help detect fraud.

3.4. Proposed System Algorithm

To improve fraud detection efficiency, the proposed system integrates machine learning algorithms with automated data processing.

Input: Transaction Dataset   D = { t1, t2, t3,....,tn}

Output: Classification of transactions as Fraudulent or Legitimate

Steps:

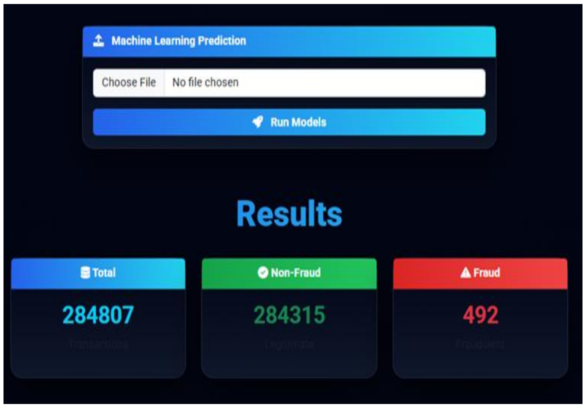
1. Load the transaction dataset.
2. Perform data preprocessing and feature extraction.
3. Split the dataset into training and testing datasets.
4. Train machine learning models using training data.
5. Evaluate model performance using testing data.
6. Predict fraud for new transactions using trained models.
7. Display fraud detection results in the dashboard.

The proposed methodology provides an effective approach for detecting fraudulent transactions by combining machine learning techniques with an interactive web-based fraud detection system.

IV. RESULTS & DISCUSSION

4.1. Dataset Processing:

The credit card transaction dataset was processed and analyzed using machine learning algorithms to detect fraudulent activities. The dataset was first uploaded through the web application interface. After uploading, the system verified the dataset structure and prepared it for further processing. The dataset contains transaction records with features that help identify whether a transaction is legitimate or fraudulent. The uploaded dataset is displayed on the web interface as shown in Figure 1.



Results

Total
284807
Transactions

Non-Fraud
284315
Legitimate

Fraud
492
Fraudulent

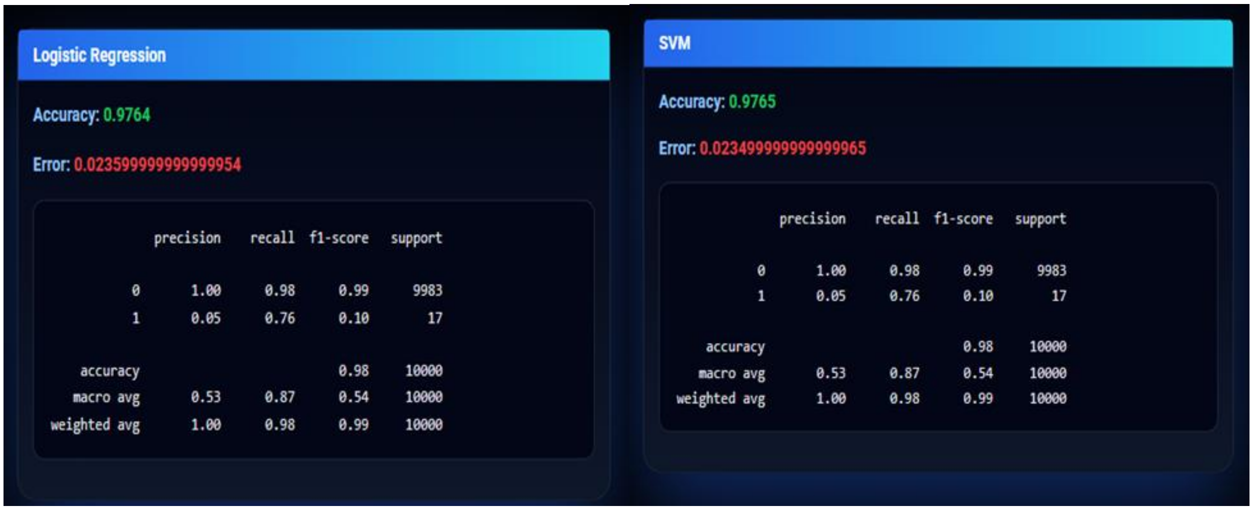
Fig 1: Dataset Upload

4.2. Data Preprocessing

Data preprocessing is performed in the code to clean and prepare the transaction dataset before training the machine learning models. The dataset is validated, features and target labels are separated, and the data is split into training and testing sets for model evaluation.

4.3. Results

The system analyzes the uploaded transaction dataset and classifies each transaction as fraudulent or legitimate using machine learning models. The results are displayed on the dashboard showing the total transactions, fraud count, and non-fraud count shown in fig 2&3.



Accuracy: 0.9764

Error: 0.023599999999999954

```
              precision    recall  f1-score   support

           0       1.00      0.98      0.99      9983
           1       0.05      0.76      0.10        17

    accuracy                           0.98     10000
   macro avg       0.53      0.87      0.54     10000
weighted avg       1.00      0.98      0.99     10000
```

Accuracy: 0.9765

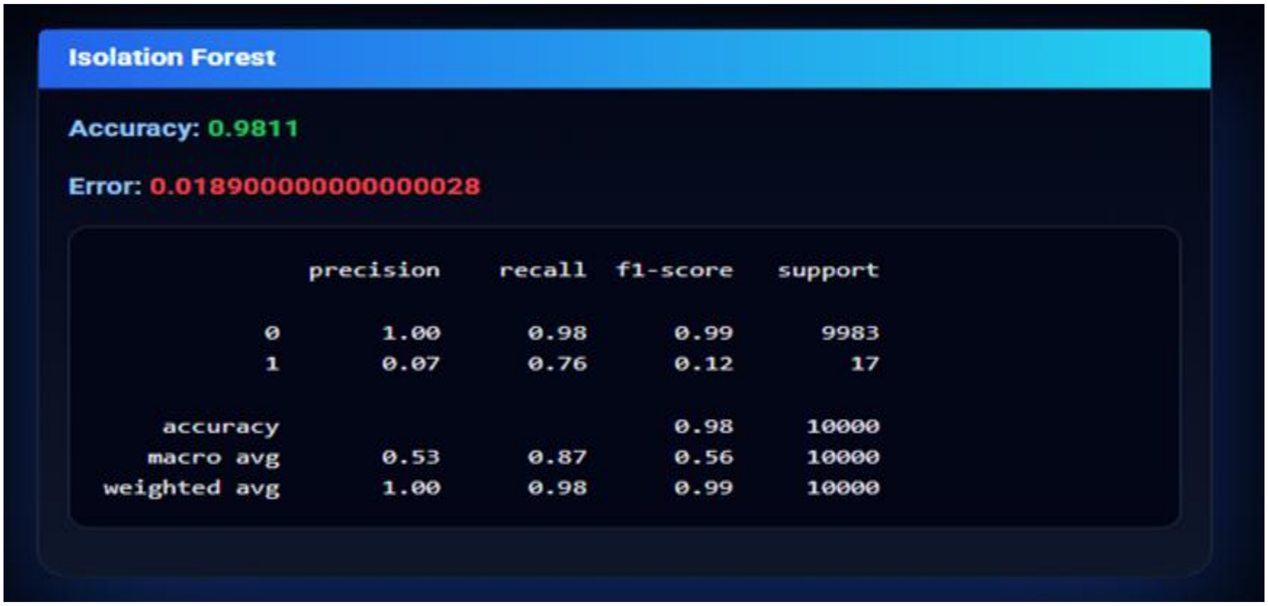
Error: 0.023499999999999965

```
              precision    recall  f1-score   support

           0       1.00      0.98      0.99      9983
           1       0.05      0.76      0.10        17

    accuracy                           0.98     10000
   macro avg       0.53      0.87      0.54     10000
weighted avg       1.00      0.98      0.99     10000
```

Fig 2: Result for Logistic Regression and Support Vector Machine



Accuracy: 0.9811

Error: 0.018900000000000028

```
              precision    recall  f1-score   support

           0       1.00      0.98      0.99      9983
           1       0.07      0.76      0.12        17

    accuracy                           0.98     10000
   macro avg       0.53      0.87      0.56     10000
weighted avg       1.00      0.98      0.99     10000
```

Fig 3: Result for Isolation Forest

4.4. Model Performance Analysis

The performance of the models is evaluated using metrics such as accuracy and error rate. A comparison graph is generated to show the performance of Isolation Forest, SVM, and Logistic Regression models sown in Fig 4&5.

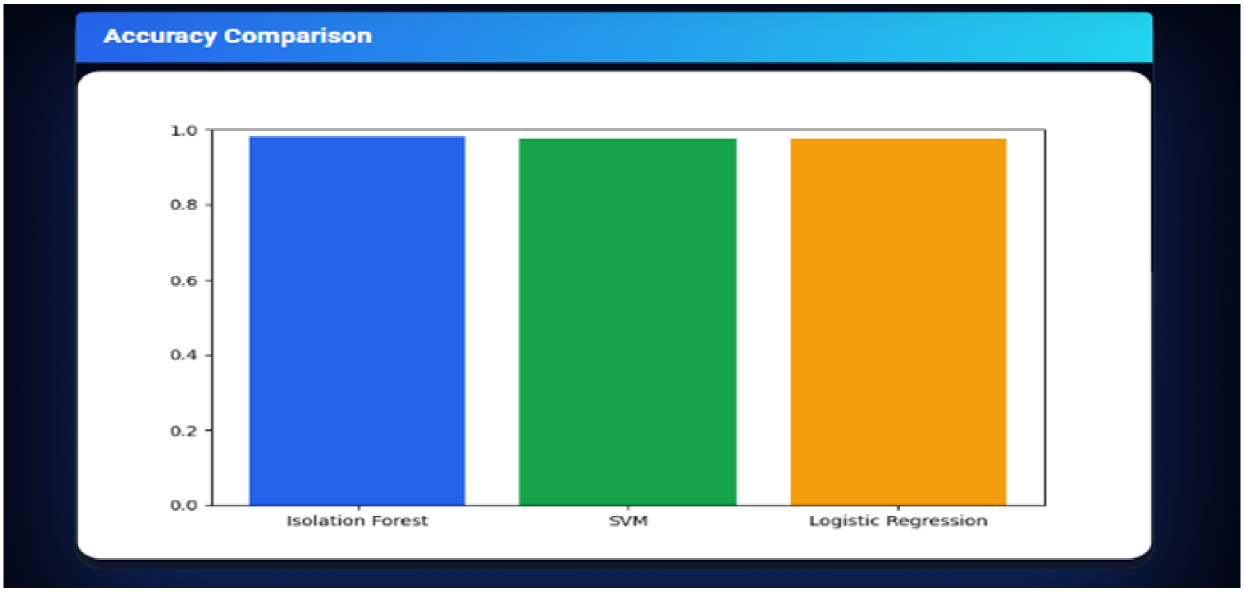


Fig 4: Accuracy Comparison

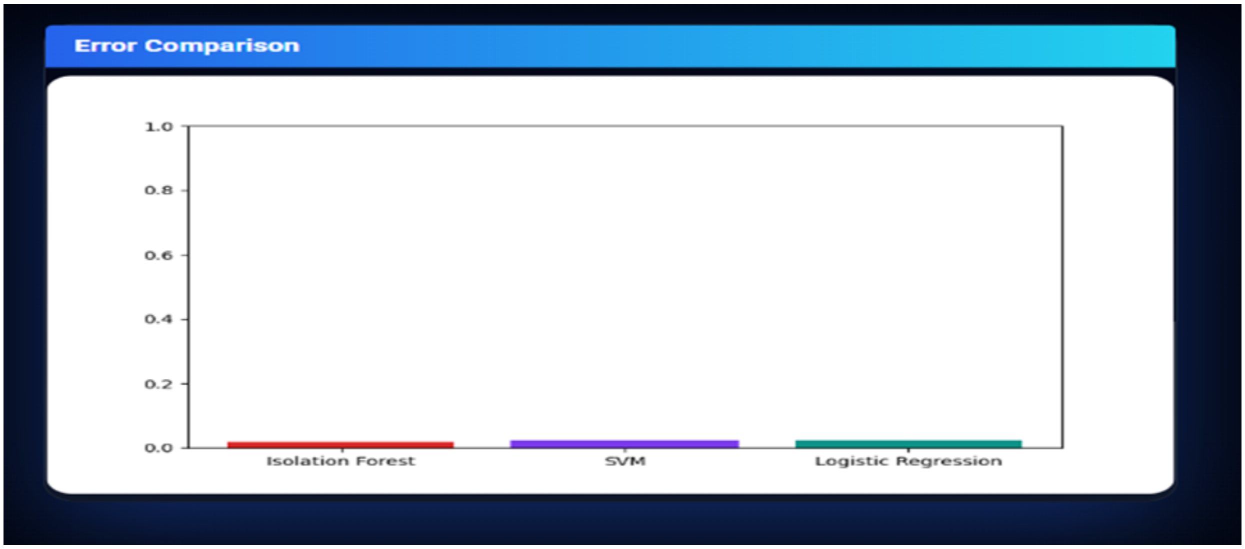


Fig 5: Error Comparison

V. CONCLUSION

Credit card fraud has become a major challenge in modern digital payment systems due to the rapid growth of online transactions and electronic commerce. This project presented a machine learning-based Credit Card Fraud Detection System designed to identify fraudulent transactions effectively. The system utilizes multiple algorithms, including Logistic Regression, Support Vector Machine (SVM), and Isolation Forest, to analyze transaction data and classify them as legitimate or fraudulent. Through data pre-processing, feature analysis, and model training, the system is able to detect suspicious patterns within transaction records. The experimental results demonstrate that machine learning techniques can significantly improve fraud detection accuracy compared to traditional rule-based systems. Furthermore, the integration of a web-based dashboard enhances the usability of the system by providing visual insights into fraud statistics, model performance, and transaction analysis. This allows users and financial analysts to monitor fraud trends and evaluate detection performance more efficiently. Although the proposed system shows promising results, challenges such as class imbalance, evolving fraud patterns, and real-time detection still require continuous improvement. Future enhancements may include the use of deep learning models, real-time streaming data analysis, and hybrid ensemble techniques to further increase detection accuracy and system reliability.

REFERENCES

[1] U. Mogili, K. V. Ampolu, B. Rajasekharam, and M. J. Timothy, "AI-Driven Interaction in AR Environments," J. Digit. Econ., vol. 3, no. 1, pp. 228–234, 2024.

[2] M. J. Timothy, B. Rajasekharam, K. V. Ampolu, and U. Mogili, "Threat Detection Using AI in Cybersecurity Systems," Int. J. Inf. Secur. (IJIS), vol. 7, no. 1, pp. 1–7, 2023.

[3] K. V. Ampolu, U. Mogili, M. J. Timothy, and B. Rajasekharam, "Machine Learning Models for Predictive Maintenance," Int. J. Inf. Secur. (IJIS), vol. 6, no. 4, pp. 1–7, 2022.

[4] B. Rajasekharam, M. J. Timothy, U. Mogili, and K. V. Ampolu, "Machine Learning Models for Predictive Maintenance," J. Digit. Econ. (JDE), vol. 2, no. 2, pp. 95–101, 2023.

[5] B. Soujania, K. V. Ampolu, M. J. Timothy, and U. Mogili, "Classifying Disease Information Forums through Semantic Similarity-Based Machine Learning," Sci. Technol. Develop. J., vol. 14, no. 2, pp. 67–75, 2025.

[6] B. S. Kumar, C. Kavitha, U. R. Mogili, and S. P. Shetty, "Application of Machine Learning To Enhance the Performance of The Prophet Routing Protocol For Delay Tolerant Networks," J. Basic Sci., vol. 23, no. 5, pp. 2107–2116, 2022, doi: 10.37896/JBSV23.5/2278.

[7] I. S. Geeta and U. Mogili, "Use of Several Machine Learning Algorithms for Effective Prediction of Cyberbullying," Int. J. Creat. Res. Thoughts, vol. 10, no. 6, p. 17, 2022.

[8] U. Mogili and A. Mohamed, "Artificial intelligence and machine learning in the fields of education, medical, and smart phones," in AIP Conf. Proc., vol. 2917, no. 1, p. 050012, Nov. 2023.

[9] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.

[10] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Stat. Sci., vol. 17, no. 3, pp. 235–249, 2002.

[11] E. W. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review," Decis. Support Syst., vol. 50, no. 3, pp. 559–569, 2011.

[12] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," Artif. Intell. Rev., vol. 34, no. 1, pp. 1–14, 2010.

[13] Y. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines," in Proc. Int. MultiConf. Eng. Comput. Scientists, 2011.

[14] A. Dal Pozzolo, O. Caelen, Y. A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Syst. Appl., vol. 41, no. 10, pp. 4915–4928, 2014.

[15] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Comput. Secur., vol. 57, pp. 47–66, 2016.

[16] F. Carcillo, Y. A. Le Borgne, O. Caelen, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," Inf. Sci., vol. 557, pp. 317–331, 2021.

[17] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed. Waltham, MA, USA: Morgan Kaufmann, 2012.

[18] S. S. D. K. M. Lakshmi, U. Mogili, S. Eluri, and D. R. Rao, "Online Dynamic Out Patient Queue System for Automated Token Generation in Hospitals," Sci. Technol. Develop. J., vol. 12, no. 7, pp. 71–78, 2023, doi: 10.18001/STD.2023.V12I07.23.37707.

[19] S. V. D. T. Sree, U. M. R. Mogili, and K. V. Ampoly, "Enhancing Security in Wearable Computing: A Lightweight Authenticated Key Exchange Scheme," Int. J. All Res. Edu. Sci. Methods (IJARESM), vol. 13, no. 5, pp. 3103–3108, 2025.

[20] S. Anjali, U. Mogili, and K. V. Ampolu, "Efficient Key-Based Encryption and Authentication for Advanced Digital Forensic Storage Security," Int. J. All Res. Edu. Sci.

Methods (IJARESM), vol. 13, no. 5, pp. 3097–3102, 2025.

[21] P. U. Adithya, U. Mogili, and J. T. Mondru, "A Novel Parity Authenticator-Based Zero-Knowledge Auditing Approach for Secure Cloud Data Management," Int. J. All Res. Edu. Sci. Methods (IJARESM), vol. 13, no. 5, pp. 994–999, 2025.

[22] K. P. Raj and U. Mogili, "Cloud-of-Cloud: A Novel Protocol for Secure Data Storage and Sharing in Multi-Cloud Environment," J. Interdiscip. Cycle Res. (JICR), vol. 12, no. 6, pp. 2201–2209, 2020, doi: 10.18001/JICR.2020.V12I6.008301.

[23] U. Mogili, A. Mohamed, and C. Kasup, "Mechanism of Data Sharing Using Secured Keyword Search in Cloud Computing," in Conf. Innov. Prod. Design Intell. Manuf. Syst., Singapore: Springer, 2023, pp. 483–494.