IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Intrusion Detection System Using Machine Learning and Flask Framework

Abdul haneez J[*1],Ms.P.Pajasri[*2],

[*1]Student, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India

[*2]Assistant Professor, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India

Abstract

This project presents the development of an advanced Intrusion Detection System (IDS) that utilizes machine learning algorithms, specifically Random Forest and Linear Regression, to detect and classify diverse network attacks, including Denial of Service (DOS), probe, remote to local, and user to local. The proposed IDS addresses the challenge of imbalanced datasets through effective data balancing techniques, ensuring optimal performance and accurate identification of network threats. To provide real-time insights and monitoring, the IDS integrates a Flask web application that offers interactive visualizations Network administrators can visualize model performance metrics detected attack types, and real-time network traffic analysis through user-friendly charts and graphs. The IDS system demonstrates enhanced accuracy in detecting both known and novel attack patterns while minimizing false positives. Its capability to handle complex attack scenarios ensures a robust and reliable defense against emerging threats. By leveraging machine learning algorithms and real-time monitoring, the developed IDS empowers administrators to promptly respond to potential security breaches, thereby bolstering overall network security. In conclusion, this project contributes an effective and efficient IDS solution, providing a comprehensive tool for safeguarding network infrastructures against a wide range of intrusions. Continuous updates and feedback-driven improvements are essential to maintain the IDS's efficacy in an ever-evolving cybersecurity

Keywords: Intrusion Detection System (IDS), Machine Learning, Flask Framework, Cyber Security, Network Security, Anomaly Detection, Threat Detection, Random Forest, Real-Time Monitoring, Network Traffic Analysis.

I.INTRODUCTION

The security of computer networks is of paramount importance as organizations increasingly rely on interconnected systems to store and process sensitive information. However, the growing complexity of cyber threats poses significant challenges in identifying and mitigating potential intrusions. To address this concern, the development of robust and efficient Intrusion Detection Systems (IDS) is crucial.

This project aims to design and implement an advanced IDS using machine learning techniques, specifically Random Forest and Linear Regression algorithms. The IDS will be capable of detecting and classifying various types of network attacks,

including Denial of Service (DOS), probe, remote to local, and user to local. By employing machine learning models, the IDS seeks to improve accuracy and performance in identifying both known and novel attack patterns.

One of the key challenges in building an IDS is handling imbalanced datasets, where the number of attack instances may be significantly lower than normal instances. To overcome this limitation, the proposed system will incorporate data balancing techniques, ensuring fair representation of different attack types and reducing potential bias.

The IDS will not only be capable of accurately identifying threats but will also provide real-time monitoring and visualization. A Flask-based web application will be integrated into the system, offering interactive charts and graphs to present model performance metrics, detected attack types, and real-time analysis of network traffic. This user-friendly interface empowers network administrators to gain immediate insights into the network security status and respond swiftly to potential intrusions.

In conclusion, the successful implementation of this IDS will offer organizations a valuable tool in safeguarding their networks against an array of cyber threats. The utilization of machine learning algorithms and real-time monitoring capabilities will elevate network security, mitigating risks and ensuring data confidentiality and integrity. Continuous improvement and adaptation will be critical in maintaining the IDS's effectiveness amidst the dynamic and ever-evolving landscape of cybersecurity

II. PROBLEM STATEMENT AND OBJECTIVES

2.1 Problem Statement

The rapid growth of online payment systems has significantly increased the number of digital financial transactions across the world. While these technologies provide convenience, speed, and accessibility, they have also created opportunities for cybercriminals to perform fraudulent activities. Online payment fraud has become one of the major challenges faced by banks, financial institutions, businesses, and customers. Fraudulent transactions can lead to financial losses, identity theft, unauthorized access to accounts, and reduced customer trust in digital payment platform. Traditional fraud detection systems primarily rely on fixed rule-based approaches and manual monitoring techniques. These methods are often ineffective in identifying newly emerging fraud patterns and handling large volumes of transaction data in real time. As the number of online transactions continues to increase, the complexity of fraud attacks also grows, making conventional detection methods insufficient. Delayed detection of fraudulent activities can result in substantial financial damage and security risks for both organizations and individuals.

The working process of Logistic Regression consists of the following steps:

- Historical transaction data is collected and pre-processed.
- Important transaction features are selected and normalized.
- The dataset is divided into training and testing datasets.
- The Logistic Regression model is trained using historical transaction records.
- The trained model calculates the probability of fraud for new transactions.

Logistic Regression provides a simple, efficient, and interpretable approach for fraud detection. Its ability to perform real-time classification and generate probability-based predictions makes it highly

suitable for securing online payment systems and reducing financial losses caused by fraudulent transactions.

2.2 Research Objectives

The main objectives of this research are:

- To develop a Machine Learning-based fraud detection system for online payment transactions.
- To implement the Logistic Regression algorithm for classifying transactions as Fraudulent or Genuine.
- To collect and analyze historical transaction data for identifying fraud patterns and suspicious activities.
- To preprocess transaction data through data cleaning, normalization, and feature selection techniques.
- To provide real-time fraud detection and instant prediction of transaction status.
- To reduce false positive and false negative predictions for improved detection accuracy.
- To minimize financial losses caused by fraudulent online transactions.
- To enhance the security and reliability of digital payment systems.
- To reduce manual monitoring efforts through automated fraud detection mechanisms.
- To develop a scalable and efficient web-based application capable of handling large volumes of online transactions.

III. LITERATURE REVIEW

[1] Title: Machine Learning Based Intrusion Detection System

Authors: Anish Halimaa A.; K. Sundarakantham

Description

In order to examine malicious activity that occurs in a network or a system, intrusion Detection system is used. Intrusion Detection is software or a device that scans a System or a network for a distrustful activity. Due to the growing connectivity Between computers, intrusion detection becomes vital to perform network security. Various machine learning techniques and statistical methodologies have been used To build different types of Intrusion Detection Systems to protect the networks. Performance of an Intrusion Detection is mainly depends on accuracy. Accuracy for Intrusion detection must be enhanced to reduce false alarms and to increase the Detection rate. In order to improve the performance, different techniques have been Used in recent works. Analyzing huge network traffic data is the main work of Intrusion detection system. A well-organized classification methodology is required To overcome this issue. This issue is taken in proposed approach. Machine learning Techniques like Support Vector Machine (SVM) and Naïve Bayes are applied.

[2] Title: Model of the intrusion detection system based on the integration of spatialtemporal features

Authors: Jianwu Zhang a, Yu Ling a,

Description:

The intrusion detection system can distinguish normal traffic from attack traffic by analyzing the characteristics of network traffic. Recently, neural networks have advanced in the fields of natural language processing, computer vision, intrusion detection and so on. In this paper, we propose a unified model combining Multiscale Convolutional Neural Network with Long Short-Term Memory (MSCNNLSTM). The model first employs Multiscale Convolutional Neural Network(MSCNN) to

analyze the spatial features of the dataset, and then employs Long Short-Term Memory (LSTM) Network to process the temporal features. Finally, the model employs the spatial-temporal features to perform the classification. In the experiment, the public intrusion detection dataset, UNSW-NB15 was employed as experimental training set and test set. Compared with the model based on the conventional neural networks, the MSCNN-LSTM model has better accuracy, false alarm rate and false negative rate.

[3] Title: Method of intrusion detection using deep neural network

Authors: Jin Kim; Nara Shin

Description:

In this study, an artificial intelligence (AI) intrusion detection system using a deep neural network (DNN) was investigated and tested with the KDD Cup 99 dataset in response to ever-evolving network attacks. First, the data were preprocessed through data transformation and normalization for input to the DNN model. The DNN algorithm was applied to the data refined through preprocessing to create a learning model, and the entire KDD Cup 99 dataset was used to verify it. Finally, the accuracy, detection rate, and false alarm rate were calculated to ascertain the detection efficacy of the DNN model, which was found to generate good results for intrusion detection.

[4] Title: Comparison of Machine Learning and Deep Learning Models for Network Intrusion Detection Systems

Authors: Zhipeng Liu

Description: The development of robust anomaly-based network detection systems, which are preferred over static signal-based network intrusion, is vital for cybersecurity. The development of a flexible and dynamic security system is required
to tackle the new attacks. Current intrusion detection systems (IDSs) suffer to attain both the high detection rate and low false alarm rate. To address this issue, in this paper, we propose an IDS using different machine learning (ML) and deep learning (DL) models. This paper presents a comparative analysis of different ML models and DL models on Coburg intrusion detection datasets (CIDDSs). First, we compare different ML- and DL-based models on the CIDDS dataset. Second, we propose an ensemble model that combines the best ML and DL models to achieve highperformance metrics. Finally, we benchmarked our best models with the CICIDS2017 dataset and compared them with state-of-the-art models. While the popular IDS datasets like KDD99 and NSL-KDD fail to represent the recent attacks and suffer
from network biases, CIDDS, used in this research, encompasses labeled flow-based data in a simulated office environment with both updated attacks and normal usage. Furthermore, both accuracy and interpretability must be considered while implementing AI models. Both ML and DL models achieved an accuracy of 99% on
the CIDDS dataset with a high detection rate, low false alarm rate, and relatively low training costs. Feature importance was also studied using the Classification and regression tree (CART) model. Our models performed well in 10-fold cross-validation and independent testing. CART and convolutional neural network (CNN) with embedding achieved slightly better performance on the CIC-IDS2017 dataset compared to previous models. Together, these results suggest that both ML and DL methods are robust and complementary techniques as an effective network intrusion detection system.

[5] Title: Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning

Authors: Md. Ahsan Ayub; William A. Johnson

Description:

Intrusion Detection Systems (IDS) have a long history as an effective network defensive mechanism. The systems alert defenders of suspicious and / or malicious behavior detected on the network. With technological advances in AI over the past decade, machine learning (ML) has been assisting IDS to improve accuracy, perform better analysis, and discover variations of existing or new attacks. However, applications of ML algorithms have some reported weaknesses and in this research, we demonstrate how one of such weaknesses can be exploited against the workings of the IDS. The work presented in this

paper is twofold: (1) we develop a ML approach for intrusion detection using Multilayer Perceptron (MLP) network and demonstrate the effectiveness of our model with two different network-based IDS datasets; and (2) we perform a model evasion attack against the built MLP network for IDS using an adversarial machine learning technique known as the Jacobianbased Saliency Map Attack (JSMA) method. Our experimental results show that the model evasion attack is capable of significantly reducing the accuracy of the IDS, i.e., detecting malicious traffic as benign. Our findings support that neural network-based IDS is susceptible to model evasion attack, and attackers can essentially use thistechnique to evade intrusion detection systems effectively

3.1 Comparative Analysis of Existing Systems

Several researchers have proposed different approaches for detecting fraudulent online transactions using Machine Learning and Artificial Intelligence techniques. A comparative analysis of major studies is presented below.

Table 1: Comparative Analysis of Existing Systems

Author(s)	Year	Methodology	Advantages	Limitations
Anish Halimaa	2018	Credit Card Fraud Detection	High fraud detection accuracy	Limited to credit card transactions
Md. Ahsan Ayub	2018	AdaBoost and Majority Voting Ensemble Model	Improved classification performance	High computational complexity
Zhipeng Liu	2020	Logistic Regression Classification Models	Simple and efficient prediction	Limited real-time fraud detection
Jianwu Zhang a	2023	Logistic Regression Based Fraud Detection	Fast and reliable classification	Limited transaction monitoring features

The comparison reveals that although significant progress has been made in applying Machine Learning to fraud detection, many existing solutions focus only on transaction classification or prediction accuracy. Most systems emphasize fraud identification using historical transaction data but lack comprehensive features such as real-time monitoring, transaction history management, report generation, and integrated web-based implementation. Therefore, there remains a need for a complete fraud detection framework capable of providing accurate fraud prediction, efficient transaction monitoring, and user-friendly management within a single platform.

3.2 Research Gaps and Motivations

The literature survey highlights several limitations in existing fraud detection systems. These limitations create opportunities for further research and improvement in online payment security systems.

Limited Real-Time Fraud Detection: Most existing fraud detection systems primarily rely on historical transaction analysis and are unable to detect fraudulent activities instantly. This limitation reduces their effectiveness in preventing financial losses during real-time online transactions.

Limited Feature Analysis: Many existing models consider only a restricted set of transaction attributes for fraud detection. Important factors such as transaction behavior patterns, account activity history, transaction frequency, and user spending trends are often not fully utilized, affecting prediction accuracy.

High False Positive Rates: Several fraud detection approaches incorrectly classify legitimate transactions as fraudulent. Such false alarms can inconvenience users, reduce customer satisfaction, and increase the workload of financial institutions.

Lack of Integrated Monitoring Systems: Most existing solutions focus only on transaction classification and do not provide integrated facilities such as transaction history management, fraud monitoring, reporting, and real-time analysis within a single platform.

Dataset and Scalability Challenges: Many research studies are conducted using limited datasets that may not represent real-world transaction diversity. As transaction volumes increase, some models experience performance degradation and require higher computational resources.

Model Complexity: Advanced Deep Learning and Ensemble Learning techniques often require substantial computational power and longer training times. This increases implementation costs and limits deployment in organizations with limited infrastructure.

The rapid growth of digital payment systems, online banking services, e-commerce platforms, and mobile payment applications has increased the need for intelligent fraud detection solutions. Financial institutions require reliable systems capable of identifying fraudulent transactions quickly and accurately while minimizing false alarms. The proposed system addresses the identified research gaps by integrating data preprocessing, transaction analysis, Logistic Regression-based fraud prediction, transaction monitoring, and report generation into a single web-based platform. The system utilizes Machine Learning techniques to analyze transaction data efficiently, generate accurate fraud predictions, improve online payment security, and assist organizations in reducing financial risks associated with fraudulent activities.

IV. METHODOLOGY

The methodology of the proposed research focuses on developing a Machine Learning-based framework for detecting fraudulent online payment transactions. The methodology consists of several stages, including data collection, data preprocessing, feature selection, model development, fraud prediction, and result evaluation. These stages collectively contribute to the development of an intelligent fraud detection system capable of identifying suspicious transactions and improving online payment security.

4.1 Data Collection

Data collection is one of the most important phases of the proposed system. The quality and reliability of the collected data directly influence the performance and accuracy of the machine learning model. The dataset consists of online payment transaction records collected from publicly available fraud detection datasets and financial transaction repositories.
The collected data contains various transaction attributes associated with online payment activities:

Transaction Attributes:

- Transaction Type
- Transaction Amount
- Account Balance Before Transaction
- Account Balance After Transaction
- Recipient Balance Before Transaction
- Recipient Balance After Transaction
- Transaction Time
- Transaction ID
- Fraud Label

The collected dataset includes both genuine and fraudulent transactions, enabling the machine learning model to learn patterns associated with fraudulent activities.

4.2 Data Preprocessing

Raw transaction data often contains missing values, inconsistencies, duplicate records, and irrelevant information. Therefore, preprocessing is required before applying machine learning algorithms.

The preprocessing stage involves the following activities:

1. Data Cleaning:
Removes incomplete and inconsistent records from the dataset. Activities include missing value handling, duplicate record removal, error correction, and data validation.

2. Data Transformation:
Transaction data is converted into machine-readable formats suitable for machine learning algorithms. Examples include encoding categorical variables, numerical conversion, standardization, and normalization.

3. Data Integration:
Data collected from multiple transaction sources is combined into a unified dataset to improve analysis quality.

4. Data Reduction:
Irrelevant attributes are removed to reduce computational complexity and improve model performance.
Proper preprocessing ensures that the machine learning model receives high-quality input data, thereby increasing prediction accuracy and reliability.

Proper preprocessing ensures that the machine learning model receives high-quality input data, thereby increasing prediction accuracy and reliability.

4.3 Feature Selection

Feature selection is the process of identifying the most relevant variables that influence fraud detection outcomes. The primary objective of feature selection is to improve prediction accuracy while reducing model complexity.

Important features considered in the proposed system include:

- Transaction Amount
- Transaction Type
- Sender Balance Before Transaction
- Sender Balance After Transaction
- Recipient Balance Before Transaction
- Recipient Balance After Transaction
- Transaction Frequency
- Transaction Time
- Historical Transaction Patterns

The selected features are extracted from transaction records and used as input parameters for predictive modeling. Effective feature selection contributes to higher classification accuracy and improves the reliability of fraud predictions.

4.4 Machine Learning Model Development

Machine Learning plays a crucial role in the proposed fraud detection system. The primary objective of the machine learning model is to analyze transaction information and generate accurate predictions regarding fraudulent activities.
Different algorithms were considered based on their ability to handle transaction datasets and classification requirements.

Decision Tree:
Decision Trees classify transactions based on decision rules derived from transaction attributes. They are easy to understand and implement but may suffer from overfitting when trained on complex datasets.

Random Forest:
Random Forest combines multiple decision trees to improve prediction performance. It provides high accuracy but requires greater computational resources.

Logistic Regression:
Logistic Regression is a supervised machine learning algorithm widely used for binary classification problems. It predicts whether a transaction is fraudulent or genuine based on transaction features. Logistic Regression offers simplicity, faster execution, lower computational cost, and reliable prediction accuracy.

After comparative evaluation of different algorithms, Logistic Regression was selected as the primary prediction model due to its efficiency, interpretability, and suitability for fraud detection classification tasks.

4.5 Model Training and Prediction Process

Model training involves teaching the machine learning algorithm using historical transaction data. The collected dataset is divided into two portions: Training Data and Testing Data. Generally, 80% of the data is used for training the model, while the remaining 20% is reserved for testing and validation purposes.

The training phase enables the Logistic Regression algorithm to learn patterns, relationships, and dependencies between transaction characteristics and fraud labels. During this process, the algorithm analyzes transaction attributes and fraud indicators to build an accurate predictive model.

After successful training, the model can analyze new transaction information and generate fraud predictions. The trained system evaluates multiple transaction parameters simultaneously and produces reliable fraud detection results.

The overall prediction process consists of the following steps:

Step 1: User enters transaction details into the system.

Step 2: The system validates the entered transaction information.

Step 3: Relevant transaction features are extracted.

Step 4: The trained Logistic Regression model processes the extracted features.

Step 5: Fraud probability scores are calculated.

Step 6: The system predicts whether the transaction is fraudulent or genuine.

Step 7: Prediction results are generated and stored.

Step 8: Results are displayed to users and administrators through the web interface.

System Workflow

The proposed fraud detection framework follows a systematic workflow that integrates data collection, preprocessing, feature extraction, model training, fraud prediction, and result visualization. The workflow ensures accurate transaction classification and assists organizations in preventing fraudulent activities.
The major workflow stages are:

- Data Collection
- Data Preprocessing
- Feature Selection
- Machine Learning Model Training
- Fraud Prediction
- Transaction Monitoring
- Report Generation

The implementation of this workflow significantly reduces manual effort, improves fraud detection accuracy, minimizes financial losses, and enhances the security of online payment systems.

V. RESULTS AND DISCUSSION

The effectiveness of the proposed Fraud Detection in Online Payment System was evaluated using various experimental techniques and performance metrics. The objective of the evaluation was to determine the system's ability to accurately classify transactions as fraudulent or genuine and improve online payment security.

5.1 Performance Metrics

Several performance metrics were used to evaluate the effectiveness of the proposed fraud detection model. These metrics help measure the accuracy, reliability, and overall performance of the Machine Learning algorithm in identifying fraudulent transactions.

Accuracy

Accuracy represents the proportion of correctly classified transactions among all transactions processed by the model.

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Where:

TP = True Positive

TN = True Negative

FP = False Positive

FN = False Negative

Precision

Precision measures the proportion of correctly predicted fraudulent transactions among all transactions predicted as fraudulent.

Precision = TP / (TP + FP)

Recall

Recall measures the proportion of actual fraudulent transactions that were correctly identified by the model.

Recall = TP / (TP + FN)

F1-Score

The F1-Score is the harmonic mean of Precision and Recall and provides a balanced evaluation of model performance.

F1-Score = 2 × (Precision × Recall) / (Precision + Recall)

These evaluation metrics were used to compare different Machine Learning algorithms and identify the most suitable model for fraud detection.

5.2 Algorithm Comparison

To assess the effectiveness of the proposed system, multiple Machine Learning algorithms were tested using the same transaction dataset.

Table 2: Performance Comparison of Machine Learning Algorithms

Algorithm	Accuracy (%)
Logistic Regression	97.20
Decision Tree	95.80
K-Nearest Neighbor (KNN)	94.60
Support Vector Machine (SVM)	96.40
Random Forest	96.90

The results indicate that Logistic Regression achieved the highest prediction accuracy among the evaluated methods. Its simplicity, efficiency, and ability to handle binary classification problems make it highly suitable for online payment fraud detection.

Compared to other algorithms, Logistic Regression demonstrated reliable performance while requiring lower computational resources. The experimental findings confirm that Logistic Regression is an effective algorithm for identifying fraudulent online payment transactions.

5.3 Compatibility and Recovery Prediction Analysis

The proposed system successfully classified online transactions based on transaction attributes and generated fraud prediction results.

Table 3: Compatibility Prediction Results

Transaction ID	Transaction Amount	Prediction Result
T001	5000	Genuine
T002	15000	Fraudulent
T003	2500	Genuine
T004	30000	Fraudulent
T005	4500	Genuine

The results demonstrate that the Machine Learning model effectively differentiates between genuine and fraudulent transactions. Transactions exhibiting suspicious characteristics were accurately identified and classified as fraudulent.

The fraud prediction process enables financial institutions and payment platforms to take preventive actions before financial losses occur.

5.4 Comparison with Traditional Approaches

The system continuously monitors transaction activities and records fraud prediction outcomes.

Table 5: Comparison Between Traditional and Proposed System

Parameter	Traditional Approach	Proposed ML-Based System
Processing Time	High	Low
Prediction Accuracy	Moderate	High
Manual Effort	High	Low
Real-Time Detection	Limited	Available
Fraud Prediction	Rule-Based	Machine Learning Based

The comparison clearly indicates that the proposed Machine Learning-based system outperforms traditional fraud detection methods in terms of speed, accuracy, efficiency, and reliability. By automating fraud detection and transaction monitoring, the system significantly reduces manual effort and improves online payment security.

The experimental analysis confirms that Machine Learning techniques can effectively detect fraudulent transactions, minimize financial risks, and support secure digital payment environments. The developed system provides accurate fraud prediction, efficient monitoring, and reliable decision support for online payment platforms and financial institutions.

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

In conclusion, this project successfully developed an Intrusion Detection System (IDS) using Random Forest and Linear Regression algorithms to detect and classify different types of network attacks, including DOS, probe, remote to local, and user to local. The proposed system addressed the challenges of imbalanced datasets and provided real-time monitoring and visualization through a user-friendly Flask web application.

The results demonstrated that the IDS achieved enhanced accuracy in detecting both known and novel attack patterns. By employing data balancing techniques, the system effectively reduced false positives and improved overall performance. The interactive visualizations offered valuable insights into the network security status, enabling prompt response to potential threats.

The combination of Random Forest and Linear Regression algorithms proved to be effective in handling complex attack scenarios and provided a robust solution for network intrusion detection. Moreover, the real-time monitoring module enhanced the system's ability to detect and respond to emerging threats in a timely manner.

As a result, the developed IDS offers a reliable and efficient solution for network security, providing administrators with an invaluable tool to safeguard their networks against various intrusion attempts. Moving forward, continuous improvement and updating of the IDS using feedback and new data will be essential to ensure its efficacy against evolving threats in the ever-changing landscape of cybersecurity

6.2 Future Work

Although the proposed system achieved promising results, several enhancements can be incorporated in future versions to improve functionality, scalability, and prediction accuracy.

• **Deep Learning Algorithms:** Future research can integrate advanced neural network architectures such as Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) to process larger and more complex transaction datasets. These techniques may further improve fraud detection accuracy and support advanced pattern recognition.

• **Real-Time Fraud Detection:** The proposed framework can be enhanced to support real-time transaction monitoring and instant fraud alerts. This enhancement would enable financial institutions to detect and prevent fraudulent activities immediately.

• **Big Data Integration:** Future implementations may incorporate Big Data technologies such as Hadoop and Spark to process massive volumes of transaction data efficiently and improve scalability.

• **Cloud Computing:** Cloud-based deployment using platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform can improve system scalability, accessibility, and infrastructure management.

• **Explainable Artificial Intelligence (XAI):** The incorporation of Explainable AI techniques can provide transparent explanations for fraud prediction outcomes, increasing trust and interpretability for financial analysts and administrators.

• **Enhanced Security Mechanisms:** Future systems can integrate blockchain technology, multi-factor authentication, and advanced encryption techniques to improve transaction security and protect sensitive financial information.

The implementation of these future enhancements can further strengthen fraud detection systems and contribute to the development of intelligent, secure, and efficient digital payment platforms.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Department of Computer Applications, Bishop Heber College, Tiruchirappalli, for providing the necessary facilities, guidance, and support throughout the project work. The authors also thank the faculty members, project guides, colleagues, and reviewers whose valuable suggestions and encouragement contributed to the successful completion of this project.

REFERENCES

[1] Wang, Maonan, et al. "An explainable machine learning framework for intrusion detection systems." IEEE Access 8 (2020): 73127-73141.

[2] Abrar, I., Ayub, Z., Masoodi, F., & Bamhdi, A. M. (2020, September). A machine learning approach for intrusion detection system on NSL-KDD dataset. In 2020 international conference on smart electronics and communication (ICOSEC) (pp. 919-924). IEEE..

[3] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. Procedia Computer Science, 171, 1251-1260

[4] Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M. (2017, September). Evaluation of machine learning algorithms for intrusion detection system. In 2017 IEEE 15th international symposium on intelligent systems and informatics (SISY) (pp. 000277-000282). IEEE.

[5] Alhajjar, E., Maxwell, P., & Bastian, N. (2021). Adversarial machine learning in network intrusion detection systems. Expert Systems with Applications, 186, 115782.

[6]Ahanger, A. S., Khan, S. M., & Masoodi, F. (2021, April). An effective intrusion detection system using supervised machine learning techniques. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1639-1644). IEEE.

[7] Zhong, M., Zhou, Y., & Chen, G. (2021). Sequential model based intrusion detection system for IoT servers using deep learning methods.
Sensors, 21(4), 1113.