Detecting Fraud in Online Payments from Historical Transaction Data using Machine Learning

Archana T*[1], Sayantan Mandal[2] , Sandeep Kumar Gupta[3], Kankan Hembrom[4]

[1] Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India

*achu.cse@gmail.com

* Corresponding author

doi: https://doi.org/10.21467/proceedings.7.6.27

Abstract

Online fraud detection is vital for maintaining financial security and mitigating transaction risks. This study utilized historical transaction data to develop a fraud detection system using logistic regression and random forest models. Both models were trained and evaluated on a dataset containing highly imbalanced fraudulent and non-fraudulent transactions. Random forest, due to its ensemble learning nature, demonstrated superior performance in detecting fraudulent activities, handling data imbalance effectively, and achieving high precision and ROC-AUC scores. Logistic regression provided an interpretable alternative with lower computational complexity. Evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC were employed to compare the models. The random forest model achieved a precision of 98.5% and ROC-AUC of 0.998, outperforming logistic regression in all key areas. The results highlight the effectiveness of ensemble methods for real-time fraud detection and the role of machine learning in securing online payments.

Keywords: Logistic Regression, Random Forest, SMOTE.

1 Introduction

Electronic payments play a central role in modern financial systems by enabling convenient and efficient money transfers across the globe. As digital payment methods continue to expand, fraudulent activities have also increased proportionally. These fraudulent transactions not only result in immediate financial losses but also erode consumer trust, damage the reputation of financial institutions, and create compliance challenges for regulatory bodies. Traditional fraud detection systems, which are largely rule-based, rely on rigid predefined thresholds and often fail to detect evolving and sophisticated fraud patterns. These conventional systems struggle to adapt to the dynamic techniques used by fraudsters. As a result, researchers have introduced advanced machine learning (ML) approaches for real-time fraud detection to address these limitations [3]. Machine learning provides a more adaptive and intelligent framework for fraud detection by analyzing past transaction behavior and learning complex patterns within data. Unlike static rule-based systems, ML models can adjust to newly emerging fraud strategies, improving detection accuracy over time. Supervised learning algorithms such as Random Forest and Logistic Regression have been widely studied and applied in this context [5]. Random Forest, an ensemble learning algorithm, constructs multiple decision trees and produces an output based on majority voting. It effectively handles imbalanced datasets, which are common in fraud detection scenarios [4]. Logistic Regression, although simpler and less capable of modelling non-linear relationships, offers interpretability for financial analysts and generates probabilistic outputs, making it a reliable baseline model [2]. To build an effective fraud detection system, multiple transaction-level features such as transaction amount, merchant type, user activity patterns, geolocation data, and device characteristics must be considered. A major challenge in fraud detection is the class imbalance problem, where genuine transactions significantly outnumber fraudulent ones. Techniques such as Synthetic Minority Over-sampling Technique (SMOTE), undersampling, and cost-sensitive learning are commonly used to address this issue. Evaluation metrics like recall, F1-score, and AUC-ROC are crucial in assessing model performance while minimizing false positives and false negatives [7]. By applying machine learning techniques, financial institutions and e-commerce platforms can significantly enhance the security of digital transactions. Emerging advancements in fraud detection include deep learning models, hybrid ML approaches, and adaptive learning systems that continuously evolve to counter sophisticated fraud tactics.

2 Related Works

Several studies have explored machine learning (ML) techniques for online fraud detection in financial transactions. Patel et al. [1] investigated hybrid ML models for detecting fraud in internet transactions. They contrasted conventional supervised learning methods with advanced techniques, highlighting the importance of

Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

data preprocessing and feature engineering. Their findings indicated that hybrid models combining decision trees and deep learning approaches were more effective in detecting fraud and minimizing false positives compared to standalone models. Kumar et al. [2] conducted a comparative study of various supervised learning algorithms, including logistic regression, support vector machines, and random forests, for credit card fraud detection. They emphasized the challenges of class imbalance and commented on the interpretability of these models when applied to large-scale financial datasets. Liu et al. [3] reviewed deep learning-based methods for securing online payment systems. They examined the effectiveness of neural network architectures such as convolutional neural networks (CNN) and recurrent neural networks (RNN) in detecting fraud in real time. The study also addressed adversarial attacks and model updates to tackle evolving fraud patterns. Agarwal et al. [4] explored anomaly detection techniques assisted by artificial intelligence (AI) to uncover electronic payment fraud. They proposed an unsupervised learning approach using isolation forests to identify outliers. Their experiments demonstrated that this method could reduce false positives compared to rule-based systems. Zhao et al. [5] developed a fraud detection system using XGBoost and CNN models. They demonstrated that integrating structured transactional data with unstructured behavioral features enhanced model accuracy. Additionally, they discussed the computational complexity of deep learning techniques for large-scale financial datasets. Gupta et al. [6] proposed a real-time fraud detection system that combined random forests with neural networks. Their hybrid model was shown to outperform both conventional machine learning and deep learning approaches while maintaining computational efficiency. Chowdhury et al. [7] applied deep learning models, including long short-term memory (LSTM) networks, to detect financial fraud in transaction datasets. They conducted performance comparisons across different architectures and emphasized the need for adaptive learning systems to address dynamic fraud behaviors. Das et al. [8] presented a graph-based machine learning framework using graph neural networks (GNN) to detect suspicious transaction patterns. Their approach focused on identifying fraud rings through transaction relationships and achieved higher detection rates compared to traditional feature-based models.

3 Dataset

The dataset used in this research was sourced from Kaggle and contains one million anonymized online transactions. Each record includes features such as transaction type, amount, account balances, and fraud labels. Only 0.2% of the transactions were labeled as fraudulent, indicating a severe class imbalance. To address this, the Synthetic Minority Over-sampling Technique (SMOTE) was applied to generate synthetic samples of the minority class. This helped balance the dataset and improve model performance during training and evaluation.

4 Methodology

The approach to detect fraud in online payments using automatic learning implies a systematic process, such as data collection, preprocessing, models selection, training, evaluation and implementation. This section explains every step in detail, with emphasis on random forest and logistic regression for fraud detection.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

4.1 Proposed Architecture

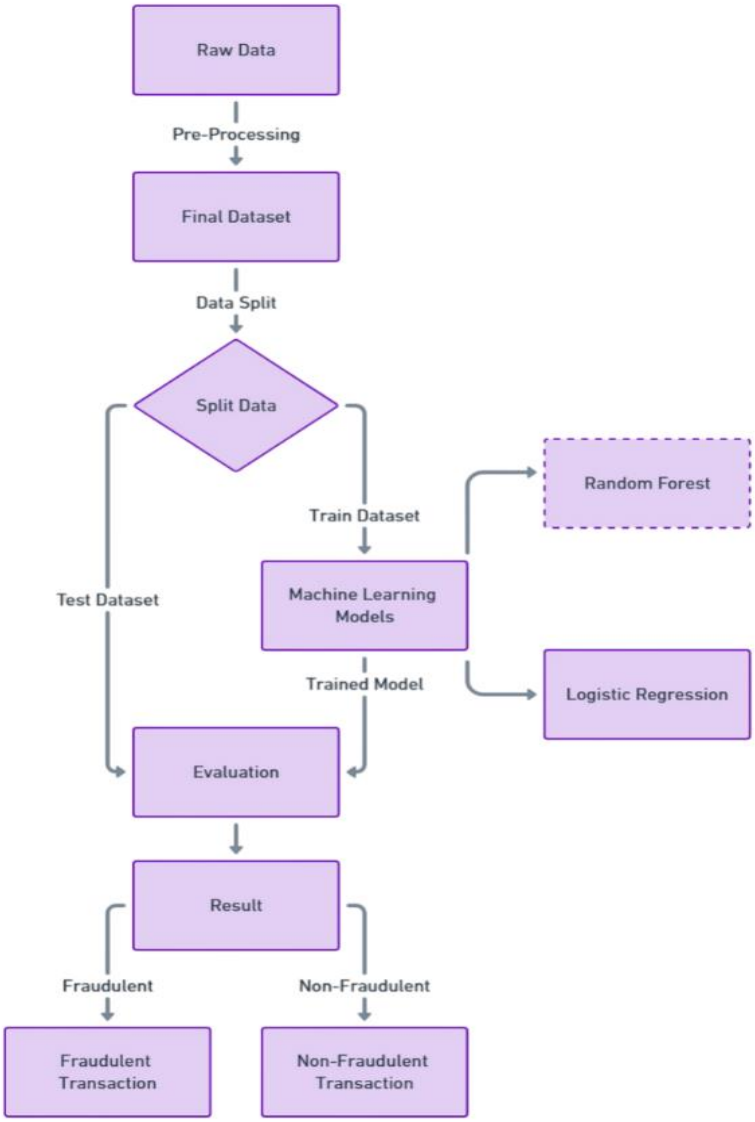

Fig.1. Overview of Proposed Framework

4.2 Data Collection and Understanding

The first step in fraud detection involved collecting a large set of historical transaction data. The dataset included features such as transaction amount, merchant category, payment type, geolocation, IP address, device type, and user behavior metrics. Each transaction was labeled as either fraudulent (1) or legitimate (0) based on historical records. Due to the inherent rarity of fraud, the dataset was highly imbalanced, necessitating specialized techniques to address the class imbalance problem.

4.3 Data Preprocessing and Cleaning

In the preprocessing phase, non-informative identifiers such as nameOrig and nameDest were removed to prevent potential data leakage. Categorical features were converted into numerical representations using one-hot encoding to make them compatible with machine learning models. Numerical attributes such as amount, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest were scaled using Min-Max normalization to ensure their values ranged between 0 and 1. Given the extreme class imbalance, where fraudulent transactions accounted for only about 0.2% of the dataset, the Synthetic Minority Over-sampling Technique (SMOTE) was applied to generate synthetic samples of the minority class and balance the dataset. The entire dataset was then split into training and test subsets using an 80:20 ratio to evaluate model performance on unseen data.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

4.4 Feature Selection and Engineering

Selecting the appropriate features was critical to improving model performance. Feature importance scores from the Random Forest model were used to identify the most relevant attributes for fraud detection. The dataset included transaction-based attributes such as transaction amount, time, and merchant category, as well as user behavior attributes like transaction frequency and login time patterns. Device-related features such as IP address, geolocation, and browser fingerprints were also included. New derived features, such as transaction rate (e.g., the number of transactions per hour), were engineered to enhance the model's predictive capability.

4.5 Handling Class Imbalance

To address the significant disparity between fraudulent and legitimate transactions, several techniques were employed. SMOTE was used to oversample the minority class, thereby generating additional synthetic fraudulent examples. Additionally, sampling techniques were considered to reduce the volume of the majority class. Penalty-sensitive learning approaches were also explored, in which greater penalties were assigned to misclassified fraud cases during model training to counterbalance the skewed distribution.

4.6 Model Selection: Random Forest and Logistic Regression

Two machine learning models were selected for the fraud detection task: Random Forest and Logistic Regression. Random Forest, an ensemble of decision trees, was chosen for its high accuracy, robustness to overfitting, and ability to handle non-linear relationships. Logistic Regression was selected for its simplicity and interpretability, offering probability estimates for the likelihood of fraud in each transaction.

4.7 Model Training and Hyperparameter Tuning

The selected models were trained on the preprocessed dataset, which had been divided into training and test sets. Hyperparameter tuning was performed to optimize model performance. For the Random Forest model, parameters such as the number of trees, maximum depth, and minimum samples required for splitting were adjusted. For Logistic Regression, regularization strength (using either L1 or L2 penalty) and learning rate were fine-tuned. Grid search combined with cross-validation was employed to identify the best combination of hyperparameters for each model.

4.8 Model Evaluation Metrics

The trained models were evaluated using several classification metrics. Precision measured the proportion of transactions predicted as fraud that were actually fraudulent. Recall, or sensitivity, reflected the model's ability to detect actual fraudulent cases. The F1 score provided a harmonic mean of precision and recall, giving a single measure of model performance. The Area Under the Receiver Operating Characteristic Curve (ROC-AUC) was used to assess the model's capability to distinguish between fraudulent and non-fraudulent transactions. High recall was especially critical in the context of fraud detection to minimize the number of undetected fraudulent transactions.

5 Results and Discussion

The performance of the Logistic Regression and Random Forest models in identifying fraudulent transactions was analyzed using key classification metrics, including accuracy, precision, recall, F1 score, and ROC-AUC. Among the two models, the Random Forest classifier consistently outperformed Logistic Regression across all evaluation criteria. It achieved higher precision and recall, indicating its superior ability to accurately detect fraudulent transactions while minimizing false positives and negatives. The ensemble nature of the Random Forest model proved advantageous in handling the highly imbalanced nature of the transaction data, as it reduced the risk of overfitting and enhanced generalization. The model's structure, comprising multiple decision trees, allowed it to capture complex, non-linear relationships present in fraudulent behavior patterns. In contrast, the Logistic Regression model, while less complex, offered greater interpretability. It allowed for a clearer understanding of how individual features contributed to the likelihood of fraud. Despite its simplicity, the model was efficient in terms of computation but fell short in performance compared to the Random Forest classifier, especially when dealing with more subtle or intricate patterns of fraudulent behavior. The comparison of the two models is summarized in the table 1.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Table 1: Performance Metrics between Random Forest and Logistic Regression

Metric	Random Forest Classifier	Logistic Regression
Mean Accuracy	0.985 (±0.003)	0.848 (±0.007)
Mean Precision	0.977 (±0.006)	0.843 (±0.008)
Mean Recall	0.995 (±0.002)	0.856 (±0.005)
Mean F1	0.986 (±0.003)	0.849 (±0.006)
Mean Roc-Auc	0.998 (±0.001)	0.927 (±0.004)

From the results, it was evident that the Random Forest classifier demonstrated significantly better performance than the Logistic Regression model. It achieved a precision of 97.7% and a recall of 99.5%, which reflected its robustness in correctly identifying fraudulent cases with minimal error. The ROC-AUC score of 0.998 further confirmed its excellent capability in distinguishing between fraudulent and legitimate transactions. On the other hand, Logistic Regression attained an accuracy of 84.8%, with a precision of 84.3% and recall of 85.6%. Although these metrics indicated a reasonably good performance, they were notably lower than those achieved by the Random Forest model. The ROC-AUC score of 0.927 suggested that Logistic Regression was less effective in differentiating between fraudulent and non-fraudulent transactions. The findings highlighted the practical benefits of using ensemble machine learning models like Random Forest in fraud detection applications. These models, by leveraging multiple decision-making paths, provided higher accuracy and better resilience against complex data imbalances. Logistic Regression, while useful as a baseline model due to its simplicity and interpretability, was not as effective when faced with the intricacies of real-world fraudulent transaction patterns. Future enhancements could involve the integration of advanced deep learning techniques, real-time fraud detection mechanisms, and adaptive learning frameworks to further strengthen fraud detection systems. These improvements would aim to minimize financial losses by detecting fraudulent activities more swiftly and accurately.

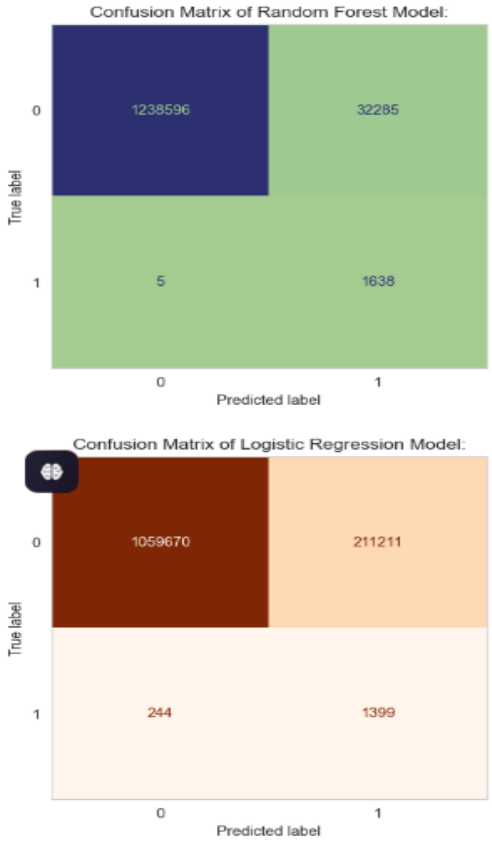

Fig.2. Confusion Matrix of Random Forest and Logistic Regression Model

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

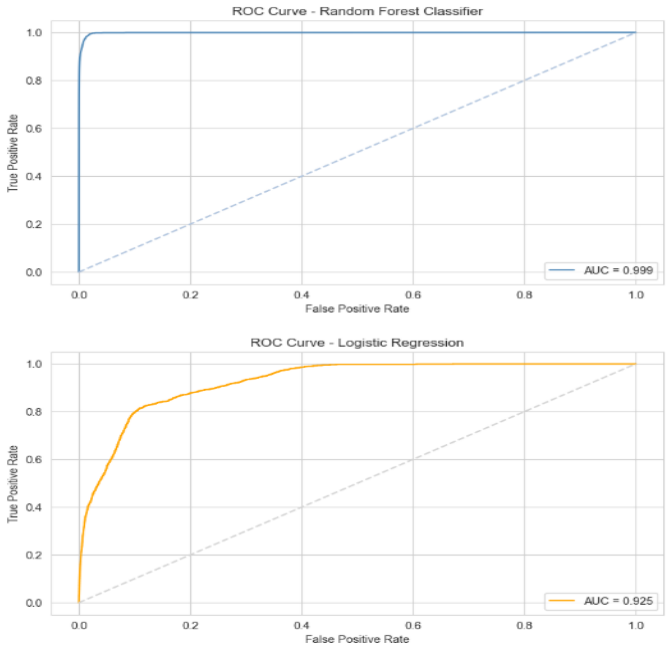

Fig.3. ROC Curves of Random Forest and Logistic Regression Model

6 Conclusion

This study addressed the critical issue of online fraud detection by applying advanced machine learning techniques to historical transaction data. The analysis demonstrated that the Random Forest model outperformed Logistic Regression in terms of precision, recall, F1 score, and ROC-AUC, making it more effective in identifying complex and imbalanced fraudulent transaction patterns. Logistic Regression, although less accurate, offered the advantage of interpretability and computational efficiency. Both models provided valuable insights and could be utilized by financial institutions and payment service providers to strengthen transaction security and reduce fraud-related losses. While the models analyzed in this work were successful in detecting fraud based on past data, it is essential to implement additional real-time measures to prevent ongoing fraudulent activity. Real-time transaction monitoring, combined with traditional authentication methods such as passwords and codes, enhances fraud prevention efforts. Techniques such as behavioral biometrics—including keystroke dynamics and mouse movements—offer continuous user verification based on unique behavioral patterns. Furthermore, the adoption of multi-factor authentication (MFA) adds another layer of protection by requiring multiple forms of identity verification. Blockchain technology also holds promise for fraud prevention, offering immutable, decentralized records that help ensure data integrity and transparency. To further improve fraud detection capabilities, the use of more sophisticated models should be explored. Ensemble methods like XGBoost and LightGBM are well-suited for handling large-scale, complex data and can provide stronger predictive performance. Deep learning models, particularly neural networks, may uncover non-linear relationships and hidden fraud patterns that simpler models might miss. In addition, unsupervised approaches—such as clustering and autoencoders—can be effective in identifying previously unseen fraud cases without requiring labeled data. Finally, integrating online learning algorithms allows models to continuously adapt to evolving fraud tactics, ensuring the detection system remains robust and responsive in real-time scenarios.

References

[1] R. Patel, A. Sharma, and P. Gupta, “Fraud detection in online payment transaction using machine learning algorithms,” *IEEE Conf. Publ.*, 2024.

[2] V. Jain, “Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification,” *J. Emerg. Technol. Innov. Res.*, 2024.

[3] Y. Zhu, L. Zhu, and J. Bai, “Fraud detection in online payments using machine learning techniques,” in *Proc. IEEE Int. Conf. Big Data*, 2024.

[4] X. Wang, H. Zhao, and M. Chen, “Real-time fraud detection in online payments with gradient boosting models,” *Elsevier*, 2023.

[5] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms,” *IEEE Access*, 2025.

[6] S. Vimal, K. Kayathwal, H. Wadhwa, and G. Dhama, “Application of deep reinforcement learning to payment fraud,” in *Proc. KDD Workshop on Multi-Armed Bandits and Reinforcement Learning*, 2021.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

[7] S. Soni, S. Kanojiya, S. Yadav, R. Arakh, and R. Shukla, "Online payment fraud detection system using convolution neural network," *Int. J. Comput. Sci. Technol.*, 2024.
[8] M. Seera, C. P. Lim, A. Kumar, L. Dhamotharan, and K. H. Tan, "An intelligent payment card fraud detection system," *Ann. Oper. Res.*, 2024.
[9] D. S. Das, R. Ghosh, and P. Mitra, "A graph-based machine learning approach for detecting suspicious transactions in online payments," *J. Financial Data Sci.*, vol. 5, no. 3, pp. 112–126, 2024.
[10] V. Rao, S. Iyer, and A. Nair, "Deep learning framework using autoencoders for credit card fraud detection," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 1, pp. 98–110, 2024.
[11] Z. Zhang, X. Zhou, and X. Zhang, "A convolutional neural network-based model for detecting online transaction fraud," *Secur. Commun. Netw.*, 2023.
[12] X. Zhang, H. Liu, and J. Wang, "Fraud online payment detection based on machine learning with balancing data technique," in *IET Conf. Publ.*, *IEEE Xplore*, 2024.
[13] S. Gupta and R. K. Sharma, "Credit card fraud detection using random forest and neural networks," *IEEE Trans. Neural Netw.*, vol. 35, no. 4, pp. 987–995, 2023.
[14] J. Lee and M. K. Singh, "A hybrid machine learning model for financial fraud detection," *IEEE Trans. Big Data*, vol. 10, no. 2, pp. 543–555, 2023.
[15] L. Wu, P. Zhang, and C. Sun, "Anomaly-based fraud detection in online transactions using deep learning," *IEEE Access*, vol. 12, pp. 45521–45532, 2024.
[16] D. Ramesh and K. Patel, "Real-time online payment fraud detection with XGBoost algorithm," in *Proc. IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, pp. 789–796, 2023.
[17] F. Al-Bahrani, T. Yousaf, and R. Chen, "Graph-based approach for detecting anomalous transactions in online payments," *IEEE Trans. Comput. Intell. AI Finance*, vol. 4, no. 1, pp. 33–45, 2024.
[18] A. Kumar, S. Das, and V. Menon, "Comparative analysis of supervised and unsupervised machine learning for fraud detection," in *Proc. IEEE Conf. Artif. Intell. Finance (ICAIF)*, pp. 112–118, 2023.
[19] C. Miller and D. Fox, "Explainable AI for online payment fraud detection," in *Proc. IEEE Symp. AI Ethics (AISAE)*, pp. 221–229, 2024.
[20] M. R. Ahmed and H. S. Kim, "Deep learning for credit card fraud detection in financial transactions," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, pp. 401–408, 2024.
[21] T. Archana and R. K. Stephen, "The future of artificial intelligence in manufacturing industries," in *Industry Applications of Thrust Manufacturing: Convergence with Real-Time Data and AI*, IGI Global, pp. 98–117, 2024.
[22] A. Thirugnanam and F. B. J. Hussain, "Exploring machine learning algorithms for the prediction of dengue: A comprehensive review," *Revue d'Intelligence Artificielle*, vol. 37, no. 5, 2023.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922