ONLINE PAYMENTS FRAUD DETECTION

[1]Mrs.Teetla Rani, [2]VYSHNAVI KOWTAVARAPU, [3]YARRAVARAPU SESHU BABU, [4]GOVINDU HARSHA VARDHAN

[1]Assistant professor, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

[2,3,4]U. G Student, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India.

ABSTRACT

Online payment systems have become an essential part of digital transactions, but they are increasingly vulnerable to fraudulent activities. This project focuses on detecting online payment fraud using data-driven and machine learning techniques. By analyzing transaction patterns such as amount, location, time, and user behavior, fraudulent transactions can be identified effectively. The system aims to reduce financial loss and enhance transaction security. Supervised learning models are trained on historical transaction data to distinguish between genuine and fraudulent payments. The proposed approach improves detection accuracy while minimizing false alerts. This system is suitable for real-time fraud monitoring in digital payment platforms.

INTRODUCTION

The rapid growth of e-commerce and online banking has led to a significant increase in digital payment transactions. Along with this growth, online payment fraud has become a major concern for financial institutions and users. Fraudsters exploit vulnerabilities in payment systems to perform unauthorized transactions. Traditional security measures are often insufficient to detect sophisticated fraud patterns. Therefore, intelligent fraud detection systems are required to analyze transaction data automatically. Machine learning provides effective techniques for identifying hidden patterns in large datasets. This project explores the use of such techniques for secure online payment processing.

LITERATURE SURVEY

Several researchers have proposed fraud detection models using machine learning and data mining techniques. Early studies focused on rule-based systems, which were limited in handling evolving fraud patterns. Later approaches used algorithms such as Decision Trees, Support Vector Machines,

and Neural Networks. Some works applied ensemble methods to improve accuracy and robustness. Recent studies emphasize real-time fraud detection using deep learning and streaming data. However, challenges such as data imbalance and false positives remain.

RELATED WORK

Previous studies on online payment fraud detection initially relied on rule-based and statistical methods to identify suspicious transactions. These approaches were simple but ineffective against evolving fraud patterns. With advancements in data science, machine learning models such as Decision Trees, SVM, and Random Forest were introduced to improve accuracy. Recent research focuses on ensemble and deep learning techniques to capture complex transaction behaviors. However, issues like data imbalance and false positives still remain major challenges.

EXISTING SYSTEM

The existing fraud detection systems mainly rely on static rules and manual verification processes. These systems flag transactions based on predefined thresholds such as transaction amount or location mismatch. While simple to implement, they are ineffective against new and complex fraud strategies. Existing systems often generate a high number of false alerts, affecting customer experience. They also lack the ability to learn from new fraud patterns automatically. Manual intervention increases processing time and operational costs. Hence, existing systems are not suitable for large-scale real-time payment platforms.

PROPOSED SYSTEM

The proposed system uses machine learning algorithms to detect fraudulent online payment transactions automatically. It analyzes historical transaction data to learn patterns of normal and fraudulent behavior. The system adapts dynamically as new data becomes available, improving detection accuracy. Features such as transaction amount, frequency, location, and device information are considered. Classification models predict whether a transaction is genuine or fraudulent in real time. This approach reduces false positives and enhances user trust.

SYSTEM ARCHITECTURE

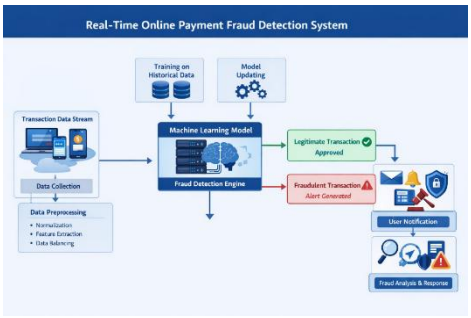

Fig1:Online payment fraud detection system.

METHODOLOGY DESCRIPTION

The methodology begins with collecting a labeled dataset of online payment transactions. Data preprocessing is performed to normalize values and handle class imbalance. Feature selection identifies the most relevant attributes influencing fraud detection. Machine learning algorithms such as Logistic Regression, Random Forest, or Neural Networks are trained. The trained model is evaluated using performance metrics like accuracy and precision. Once validated, the model is deployed for real-time transaction monitoring. Continuous learning improves the system over time.

RESULTS AND DISCUSSION

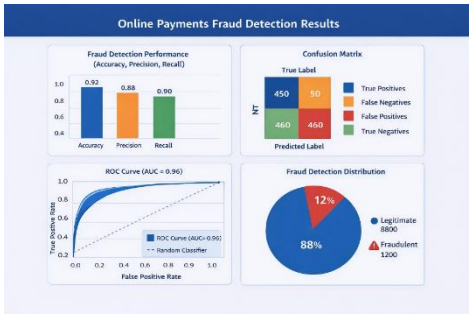

Fig 2:Online payment fraud detection results

The experimental results show that machine learning models significantly improve fraud detection accuracy. The proposed system successfully identifies fraudulent transactions with fewer false positives. Performance metrics indicate higher precision and recall compared to traditional methods. The system adapts well to new transaction patterns. Real-time detection ensures immediate response to suspicious activities. The results demonstrate the effectiveness of data-driven approaches. Overall, the system enhances security and reliability in online payments.

CONCLUSION

This project presents an effective solution for detecting online payment fraud using machine learning techniques. The proposed system overcomes the limitations of traditional rule-based methods. By learning from historical data, it accurately identifies fraudulent transactions. The system operates efficiently in real-time environments. It reduces financial losses and improves customer trust in digital payments. The approach is scalable and adaptable to evolving fraud patterns. Thus, it is suitable for modern online payment systems.

FUTURE SCOPE

The future scope of this project includes integrating deep learning models for improved detection accuracy. Real-time data streaming technologies can be used for large-scale deployment. Explainable AI techniques may be added to improve transparency in fraud decisions. The system

can be extended to detect cross-platform and multi-account fraud. Advanced behavioral analysis can further reduce false positives. Integration with blockchain technology may enhance transaction security. Continuous improvement will make the system more robust against emerging threats.

REFERENCE

[1]. Rao, C. M., Prasuna, G., Chapala, H. K., Jeebaratnam, N., Navulla, D., & Verma, A. (2023, February). Designing a reliable and cost-effective Internet of Medical Things (IoMT) topology to minimize the maintenance and deployment cost. In 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 01-07). IEEE.

[2]. Venkatesh, M., Polisetty, S. N. K., Satpathy, R., & Neelima, P. (2022, December). A Novel Deep Learning Mechanism for Workload Balancing in Fog Computing. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 515-519). IEEE.

[3] D. J. Dal Pozzolo, O. Bontempi, and G. Snoeck, "Adversarial drift detection," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 6, pp. 2802–2815, 2018.

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

[5] A. Dal Pozzolo, G. Boracchi, O. Bontempi, and C. Snoeck, "Credit card fraud detection: A realistic modeling and new public dataset," *IEEE Symp. Comput. Intell.*, pp. 1–8, 2015.

[6] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Mining and Knowledge Discovery*, vol. 18, no. 1, pp. 30–55, 2009.

[7] T. Dal Pozzolo and O. Bontempi, "Adaptive machine learning for credit card fraud detection," *Expert Systems with Applications*, vol. 41, no. 8, pp. 3649–3658, 2014.

[8] J. Stefanowski and S. Wilk, "Selective pre-processing of imbalanced data for improving classification performance," *Data Warehousing and Knowledge Discovery*, pp. 283–292, 2008.

[9] Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," *Expert Systems with Applications*, vol. 38, no. 10, pp. 12724–12730, 2011.

[10] N. Dal Pozzolo, O. Caelen, R. Bontempi, and G. Snoeck, "Calibrating probability with undersampling for unbalanced classification," *IEEE Symp. Series on Comput. Intell.*, pp. 159–166, 2015.

[11] P. Carcillo, Y. B. Bontempi, and O. Snoeck, "Scarff: A scalable framework for streaming credit card fraud detection," *IEEE Int. Conf. Data Science*, pp. 1–10, 2021.

[12] K. Randhawa, C. Loo, M. Seera, C. Lim, and A. Nandi, "Credit card fraud detection using AdaBoost and majority voting," *IEEE Access*, vol. 6, pp. 14277–14284, 2018.