ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Credit CardE-Commerce Fraud Detection Using Machine Learning

[1]E. Swetha,[2]S. Akhila,[3]T. Manasa,[4]S. Lakshmi,[5]K. Anitha,[6]V. Shyamala

[1]Assistant Professor, Dept of CSE, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

[2,3,4,5,6]U. G Student, Dept of CSE, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

ABSTRACT- ***The rapid growth of digital payments and e-commerce has increased the risk of fraudulent transactions, making traditional rule-based systems ineffective. This project proposes a machine learning-based fraud detection system using historical transaction data. Data preprocessing and feature engineering are applied to improve data quality and extract meaningful features. Supervised learning algorithms such as Logistic Regression, Random Forest are used to classify transactions as legitimate or fraudulent. The model learns fraud patterns from past data and adapts to new fraud techniques. Overall, the system enables early fraud detection and ensures secure and reliable digital transactions.***

KEYWORDS- ***shopping cart, product catalog, payment gateway, online payment, digital wallet, management, logistics, delivery, customer reviews, SEO, digital marketing, CRM, security, cloud computing, AI, chatbots.***

INTRODUCTION

With the advancement of technology, online shopping and digital payment methods such as credit cards, debit cards, and mobile wallets have become an integral part of everyday life, resulting in millions of transactions occurring daily across e-commerce platforms, banking systems, and financial applications. While these systems provide convenience and speed, they also introduce serious security challenges in the form of fraudulent activities, where unauthorized users perform transactions using stolen or compromised card details. Detecting such fraud manually is impractical due to the massive volume of transactions and the subtle nature of fraudulent behaviour, and fraudsters

continuously modify their strategies to bypass traditional security mechanisms. Machine Learning (ML) offers an intelligent and automated solution by analyzing historical transaction data to learn hidden patterns, detect anomalies, and classify transactions with high accuracy. This project focuses on designing an efficient fraud detection system using data science and machine learning techniques to ensure secure, reliable, and real-time transaction monitoring.

LITERARTURE SURVEY

The literature survey reviews existing research on customer churn prediction in e-commerce systems. Many studies use machine learning algorithms such as Logistic Regression, Decision Trees, and Random Forest for churn analysis. Researchers have identified customer behaviour, purchase history, and engagement levels as key factors influencing churn. Data preprocessing and feature selection are highlighted as critical steps for improving model performance. Some studies explore the use of deep learning for handling large and complex datasets. Several researchers focus on predictive analytics to help businesses take preventive actions. Chatbots are also studied for enhancing customer interaction and support services. Literature shows that chatbots improve user satisfaction and retention. However, most existing systems focus only on churn prediction. This project extends previous work by integrating churn prediction with chatbot interaction in a full stack web application.

EXISTING METHOD

In the existing system, customer churn management in e-commerce platforms is mostly handled manually and using traditional methods. Businesses rely on historical sales data, customer complaints, and basic statistical analysis to understand customer behaviour. Some systems use simple rule-based techniques, such as identifying customers who have not logged in or made purchases for a long time. In a few cases, traditional machine learning models are applied, but they function separately from customer interaction systems. Customer support is largely manual and depends on human representatives. Customers are usually contacted only after problems occur. There is no real-time engagement with users. Personalized communication and offers are rarely provided. These systems struggle to process large volumes of customer data efficiently. As a result, customer churn is often identified too late, leading to revenue loss.

PROPOSED METHOD

The proposed system utilizes machine learning algorithms to detect fraudulent credit card and e-commerce transactions automatically. Instead of relying on fixed rules, the system learns transaction patterns from historical data and identifies suspicious activities based on statistical and behavioural features.

The system performs data preprocessing, feature extraction, and model training using labeled transaction data. Once trained, the model can classify incoming transactions in real time. The proposed approach adapts to new fraud strategies, reduces false alerts, and provides faster and more accurate fraud detection.

SYSTEM ARCHITECTURE

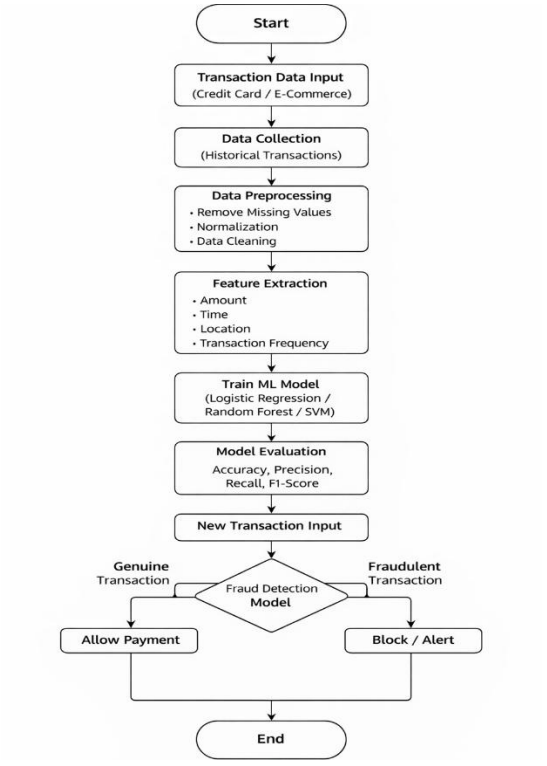

Fig 1: Block Diagram

METHODOLOGY DESCRIPTION

By using the block diagram, we can describe how customer data is collected from the e-commerce platform and processed to predict customer churn. After data collection, the customer information is analyzed using machine learning techniques. If the system correctly identifies a potential churn customer, appropriate actions are triggered; otherwise, no action is taken. The final step focuses on retaining the customer through chatbot interaction and personalized engagement.

Customer Data Input: Customer data such as purchase history, browsing behaviour, login frequency, and time spent on the website is collected.

Data Preprocessing: The collected data is cleaned by removing missing values, duplicates, and irrelevant information.

Data Transformation: The cleaned data is converted into a suitable format for machine learning analysis.

Feature Selection: Important customer behaviour features influencing churn are identified.

Model Training: Machine learning algorithms are trained using historical customer data.

Churn Prediction: The trained model predicts whether a customer is likely to churn.

Chatbot Activation: If churn is detected, an intelligent chatbot interacts with the customer in real time.

Output Display: Prediction results and chatbot interactions are displayed to administrators and recorded for monitoring.

RESULTS AND DISCUSSION

Fig: -2 Signup Page

The signup page allows new users to create an account by entering basic registration details.

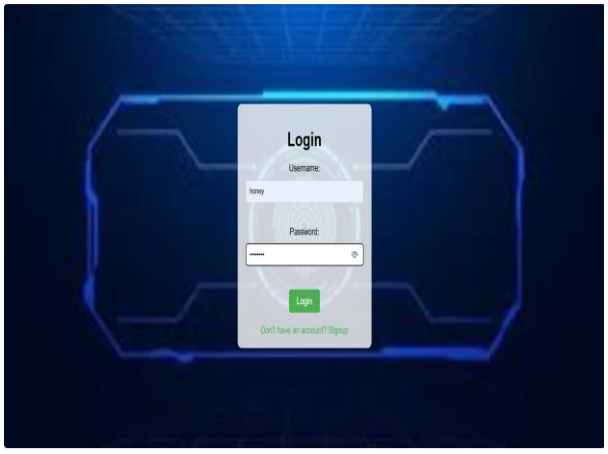

Fig: -3 Login Page

The login page enables registered users to securely access their account using valid credentials.

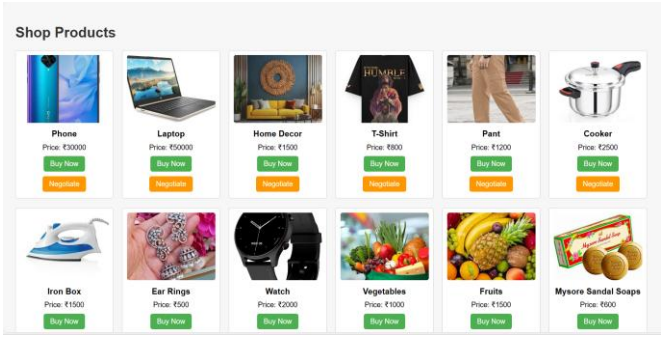

Fig: -4 Shop Page

The shop page displays available products and allows users to browse and select items for purchase.

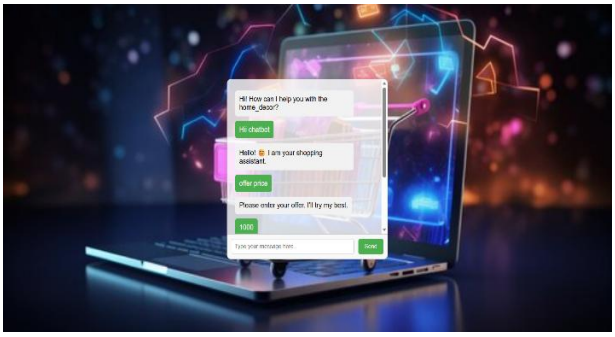

Fig: -5 Chabot Page

The chatbot interacts with users in real time, answers queries, and improves

customer engagement using NLP.

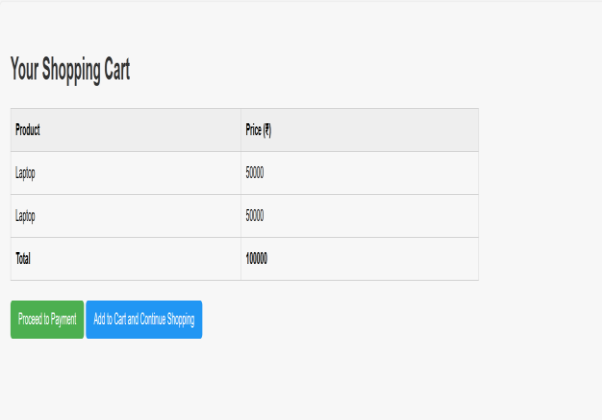

Fig: -6 Shopping Cart

The cart page shows selected products and allows users to review items before proceeding to payment.

Fig: -7 Payment Page

The payment page allows users to complete their purchase using secure transaction methods.

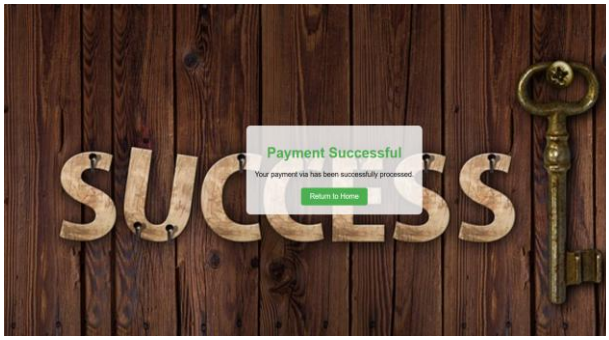

Fig: -8 Payment Success Page

This page confirms successful payment and provides transaction completion details to the user.

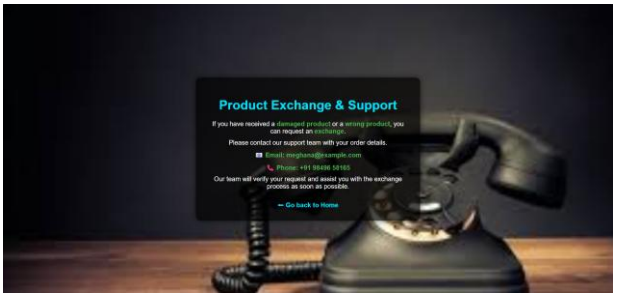

Fig: -9 Contact Page

The contact page allows users to communicate with the admin for support, feedback, or queries.

CONCLUSION

The proposed machine learning-based fraud detection system effectively identifies fraudulent transactions using Logistic Regression and Random Forest algorithms. It improves detection accuracy through data preprocessing, feature engineering, and real-time transaction analysis. The system reduces financial losses, minimizes manual intervention, and provides timely alerts for suspicious activities. Overall, it offers a scalable, reliable, and secure solution for modern digital payment and e-commerce platforms.

FUTURE SCOPE

Future improvements can include deep learning models, adaptive real-time learning, and advanced anomaly detection

techniques to enhance fraud identification. Integrating blockchain, federated learning, and explainable AI can improve security, transparency, and regulatory compliance. Cloud-native deployment and intelligent alert prioritization will increase scalability and operational efficiency. These enhancements will enable the system to adapt quickly to evolving fraud patterns while maintaining high detection accuracy.

REFERENCES

1. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.

2. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.

3. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.

4. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.

5. Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines. International MultiConference of Engineers and Computer Scientists, 1, 442–447.

6. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245.

7. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113.

8. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797.

9. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66.

10. Rashid, S., & Khan, M. (2019). Machine learning techniques for fraud detection: A review. International Journal of Advanced Computer Science and Applications, 10(3), 90–96.

11. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. Expert Systems with Applications, 51, 134–142.

12. Liu, Y., & Wu, X. (2009). Credit card fraud detection using PCA and SVM. Proceedings of the 2009 International Conference on Neural Networks and Brain, 2, 641–645.

13. Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2018). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 455, 217–229.

14. Bhatt, C., & Jani, P. (2020). Fraud detection in e-commerce using machine learning. International Journal of Engineering Research & Technology, 9(2), 124–130.

15. Hand, D. J., & Whitrow, C. (2009). Statistical challenges of fraud detection. Journal of the Royal Statistical Society: Series A, 172(2), 421–439.

16. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.

7. Patil, S., & Sherekar, S. (2013). Performance analysis of Naïve Bayes and J48 classification algorithm for data classification. International Journal of Computer Science and Applications, 6(2), 256–261.

18. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89.

19. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18, 30–55.

20. Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences, 3, 621–630.

21. Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785–794.

22. Quinlan, J. R. (1996). Improved use of continuous attributes in C4.5. Journal of Artificial Intelligence Research, 4, 77–90.

23. Wang, S., & Xu, C. (2018). Random Forest for credit card fraud detection. Proceedings of the IEEE International Conference on Big Data, 2287–2294.