



e-ISSN:2582-7219



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 8, August 2024



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521



6381 907 438



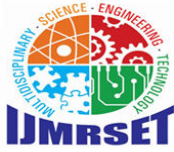
6381 907 438



ijmrset@gmail.com



www.ijmrset.com



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Detection of UPI Fake Payments using ML

Dr.Murganandham¹, Dr.T.Subburaj², Meghana.N³

Department of Master of Computer Applications, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

ABSTRACT: UPI PAYMENTS FRAUD DETECTION is an innovative python project designed from ml methodologies. This project emphasizes the crucial importance of financial institutions in detecting and preventing fraudulent acts. ML method provides a mechanism to prevent a online transaction frauds with a high accuracy.

Now-a-days there is demand for high number of online payments, leading to danger of online fraud. The intention of system is to execute SML methods for detecting frauds, from the aim of analyzing prior transaction information.

KEYWORD: Fraud, Machine Learning, Online Payments.

I. INTRODUCTION

UPI PAYMENTS FRAUD DETECTION python project was created by using SML method. Our project helps to detect the online frauds depends on the transactions made by the customers. ML approaches helps to recognize and evaluate fraud in online transactions. Now-a-days, fraud had been a major issue in each and every sector, such as remote banking, e-commerce, etc..., Due to raise in online transactions through different payments methods, like amazonpay, googlepay, paytm, phonepe, bhim, etc., fraudulent activities have also increased.

Here, the machine tries to prove itself by supplying materials and produces good results based on experience. This format is good way to check online fraud because of its fast calculation.

The project falls under the classification machine learning problem where it predicts whether the transaction is a legal or illegal. ML algorithms such as svm and rfc has been used to demonstrate the accuracy of regular operations.

II. LITERATURE SURVEY

Kenichi Yoshida and Hiroki Azuma, his paper gives an over look about remote mode of purchases Frauds Detecting Systems and its Evaluation.[1]

Simon Delecourt and Lio Guo, research paper establishes a strong MPF examine System with Adverse Examples.[2]
Nadia Boutaher and Mohammed Rida, This Journal informs an overview of platinumcard detection using ml methodology.[3]

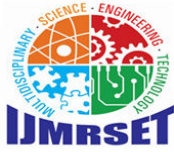
A Study of DL Based remote settlements Fraud examine Systems by Kanika and Dr Jimmy Singla.[4]

Lakshika Sammani Chandradeva and Achala Chaturanga Aponso, Journal provides data regarding detection of frauds for the monetary transactions with auto- encoders.[5]

“Improved duplicity examines in E-Commerce Transactions” by Jisha Shaji and Dakshata Panchal.[6]

III. EXISTING SYSTEM

Two ml model were put forth and executed to unveil forged transactions. Multiple gauges are utilized to evaluate the effectiveness of classifiers and predictors, such as Vector Machine, Random Forest and Decision Tree. These criteria are contingent on either prevalence or prevalence-independence. Furthermore, these methodologies are employed in upi detection of frauds, and output of these algorithms are accurate.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

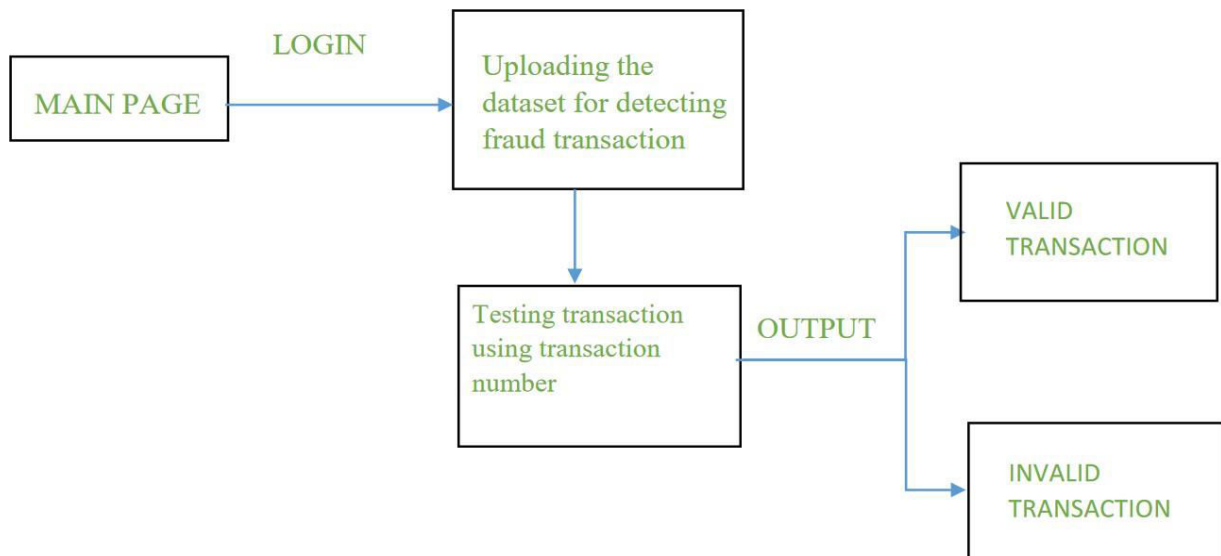
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. PROPOSE SYSTEM

The proposed system of remote transactions fraud detection aims to enhance the security and efficiency of detecting fraudulent activities in UPI transactions. The system will leverage advanced machine learning algorithms and data analytics techniques to analyze transactional data, user behavior, and transaction patterns in real-time. The key components of system include data collection, report analysis, ml models. Overall project aims to improve the security and efficiency.

V. IMPLEMENTATION

1. METHODOLOGY

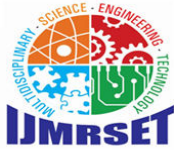


VI. RESULTS



Figure. 1: HOME PAGE

It is a main dashboard of our project. It deals with the detection of fraud transactions and major Graphical User Interface.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

UPI FRAUD DETECTION

Enter UPI number

UPI holder name

Select state

Enter the date and time of transaction

Enter Seller name

Enter date of Birth

Enter pin code

Enter transaction amount (Rs)

Select merchant category

Click to Detect

Figure.2: TESTING PAGE

In this page, we enter the data of the customer and process for testing the details of the customer for UPI fraud payments.

RESULT

VALID TRANSACTION

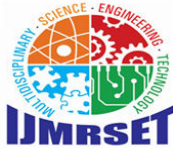
Back to Home

Figure.3: OUTPUT

After entering the data of customers, it tests the data completely and detects and fraud UPI payments and finally it gives the results of valid transaction.

VII. CONCLUSION

In Conclusion, the Unite settlement associate remarkable transformed the digital payments landscape in India, offering users a convenient and secure way to make transactions. However, the increasing popularity of UPI has also attracted the attention of fraudsters, leading to rise in fraudulent activities. To combat this, it is essential to implement robust fraud detection mechanisms that can accurately identify and prevent fraudulent transactions. Going forward, it crucial to continue innovating and enhancing fraud detection mechanisms to keep pace with the evolving fraud tactics.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. M. A. Pavaskar and K. K. Tripathi, "Survey on platinumcard duplicity examine methods," *Abroad articles of Emerging Technology and Advanced Engineering*, vol. 2, no. 11, pp. 721–726, 2012.
2. S.Sural, A.Srivastava, A.Majumdar, and A.Kundu "platinumcard duplicity examine using masked markovv model,".
3. I.Sutskever, C.Szegedy, J.Bruna, W.Zaremba, D.Erhan, I.Goodfellow, and R.Fergus, "fascinate assets of NN networks," 2013.
4. D.Wagner and N.Carlini, "as regards gauge the agility of NN networks," in *2017 IEEE forum on shielding and Protecting (SP)*, pp. 39–57, IEEE, 2017.
5. I.Goodfellow, A.Kurakin and S.Bengio, "Antagonistic models in the society," *arXiv preprint arXiv:1607.02533*, 2016.
6. A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards DL methods unaffected by Antagonistic attacks," *arXiv preprint arXiv:1706.06083*, 2017.
7. P. Manoharan, K. Grosse, M. Backes, N. Papernot, and P. McDaniel, "Antagonistic models for malfunction examine," in *abroad forum on publications in software system protection*.
8. X. Wu, S. Jha, N. Papernot, A. Swami and P. McDaniel, "Refining as a shielding to antagonistic disruption opposite DN networks," in *2016 forum on shielding and protecting*, pp. 582–597, IEEE, 2016.
9. [10] P. Manoharan, K. Grosse, P. McDaniel, N. Papernot and M. Backes, "antagonistic disruption opposite DN networks for malfunction organization," ar



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com