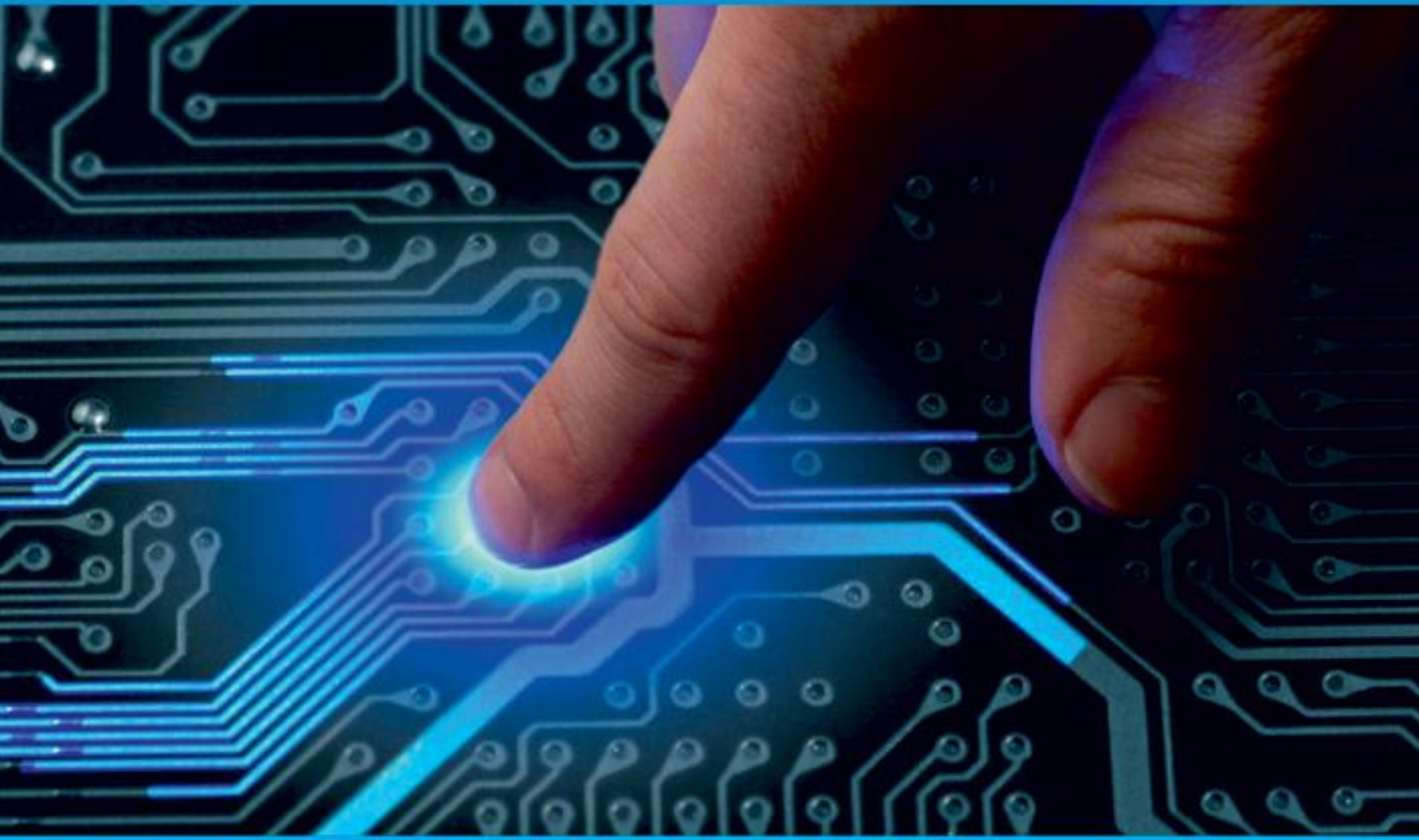
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

UPI Fraud Detection Using Cyber Security

Sanjaykumar M[1], Karthik M[2,] Mohanraj R[3], Surendarsai K[4]

Mrs.P.Jayasutha M.E[5]

Department of Computer Science Engineering, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamilnadu, India[1,2,3,4]

Assistant Professor**,** Department of Computer Science Engineering, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamilnadu, India[5]

ABSTARCT: With the rapid growth of digital transactions, the Unified Payments Interface (UPI) has emerged as a popular and convenient method for financial transactions in the modern era. However, the increasing reliance on digital platforms has also led to a rise in fraudulent activities. This paper proposes a robust UPI fraud detection system employing advanced Cyber techniques to enhance the security of digital transactions. The proposed system leverages a diverse set of features, including transactional patterns, user behavior, and device information, to create a comprehensive model for fraud detection. Cyber Security learning algorithms, such as supervised learning classifiers and anomaly detection techniques, are employed to analyse historical transaction data and identify patterns indicative of fraudulent activities. UPI service providers must ensure the security of communication channels between users and their platforms. Employing encryption protocols and regularly updating security measures helps protect user data from interception by malicious actors. Malicious software can compromise the security of UPI transactions by infiltrating a user's device and capturing sensitive information. Users may unknowingly download malware or spyware through seemingly harmless apps, making it essential to exercise caution when installing applications on devices linked to UPI accounts.

KEYWORDS: Cyber techniques, Unified Payments Interface (UPI), detection algorithm, Hidden Markov Model (HMM), UPI application.

I. INTRODUCTION

1.1 OVERVIEW

Implementing multi-factor authentication (MFA) adds an extra layer of security to UPI transactions. In addition to passwords and UPI PINs, requiring users to authenticate transactions through OTPs or biometric verification enhances security and makes it more challenging for fraudsters to gain unauthorized access.

This technology holds the potential to minimize financial losses, protect user privacy, and enhance the overall security of digital payment ecosystems. In this era of constant technological evolution, it is crucial for financial institutions, finch companies, and payment service providers to implement advanced Cyber Security models and algorithms to stay ahead of fraudsters. This approach not only helps in detecting known fraud patterns but also adapts to emerging threats through continuous learning and optimization.

This introductory chapter reviews the fundamental concepts of cyber security. It begins with common threats to information and systems to illustrate how matters of security can be addressed with methods from risk management. In the following, typical attack strategies and principles for defence are reviewed, followed by cryptographic techniques, malware and two common weaknesses in software: buffer overflows and SQL injections. Subsequently, selected topics from network security, namely reconnaissance, firewalls, Denial of Service attacks, and Network Intrusion Detection Systems, are analysed. Finally, the chapter reviews techniques for continuous testing, stressing the need for a free distribution of dual-use tools. Although introductory in nature, this chapter already addresses a number of ethical issues. For instance, well-intended security mechanisms may have undesired side effects such as leaking sensitive information to attackers. As asymmetries and externalities are at the core of many security problems, devising effective security solutions that are adopted in practice is a challenge.

it as a mainstream payment method, leading to a high volume of transactions on online trading platforms. Unfortunately, this popularity also attracts criminals who exploit the complex network environment to commit fraud. Such fraudulent activities not only harm consumers but also impede the healthy growth of the online economy. Consequently, effective transaction fraud detection becomes a vital tool in combating network transaction fraud. Traditional fraud detection approaches primarily rely on statistical and multi-dimensional analysis techniques.

However, these verification based methods struggle to uncover the underlying patterns in transaction data, limiting their effectiveness. On the other hand, big data technology and algorithms offer efficient solutions for detecting transaction fraud. , particularly when applied to large datasets, can capture important features that traditional statistical methods fail to describe. By utilizing suitable techniques, we can build models based on existing transaction data to detect network transaction fraud, thereby mitigating associated losses. In 2018, Zhaohui Zhang proposed a reconstructed feature convolutional neural network prediction model specifically tailored for transaction fraud detection. This model demonstrated improved stability and classification effectiveness compared to other convolutional neural network models. However, a challenge remains in achieving high detection accuracy due to imbalanced sample labels. To address this, the paper introduces two fraud detection algorithms: one based on a Fully Connected Neural Network and another utilizing XGBoost. The former algorithm integrates two neural network models with different cross-entropy loss functions, enabling a quick and convenient design process for the combined model.

II. LITERATURE SURVEY

1. **Review Paper on UPI Fraud Detection Using**
Authors: Miss. Sayalee S. Bodade, Prof. P.P. Pawade
Year-2021
With the rapid growth of digital transactions, the Unified Payments Interface (UPI) has emerged as a popular and convenient method for financial transactions in the modern era. However, the increasing reliance on digital platforms has also led to a rise in fraudulent activities. This paper proposes a robust UPI fraud detection system employing advanced Cyber Security techniques to enhance the security of digital transactions. The proposed system leverages a diverse set of features, including transactional patterns, user behaviour, and device information, to create a comprehensive model for fraud detection. Cyber Security algorithms, such as supervised learning classifiers and anomaly detection techniques, are employed to analyse historical transaction data and identify patterns indicative of fraudulent activities. The model is trained on a labelled dataset that includes both genuine and fraudulent transactions, ensuring its ability to distinguish between normal and suspicious behavior.

2. Online Transactions Fraud Detection using Cyber Security
Author -Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omanna, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai.
Year -2023
Now a days Digital transactions are rapidly increasing as it results in increasing online payment frauds too. In fact, according to the Reserve Bank of India, comparing March 2022 to March 2019, digital payments have risen in volume and value by 216% and 10%, respectively. People are starting to go all-in with digital transactions, but one can't deny the security issues that loom, and know-how when it comes to online payments. Few years ago, we could have barely seen the online payment, but today UPI payment QR code installed at doorstep. This invited the hoaxers and attackers to develop fraudulent transactions and fool people for some amount of money. Fortunately, the online transactions are monitored and hence could be analysed using the latest tools. In this system, an attempt is made to develop a Cyber Security model to identify fraudulent transactions in a transaction's dataset.

EXISTING SYSTEM

- ➢ To detect counterfeit transactions, three machine-learning algorithms were presented and implemented.
- ➢ There are many measures used to evaluate the performance of classifiers or predictors, such as the Gradient Boost Classifier, Vector Machine, Random Forest, and Decision Tree.
- ➢ These metrics are either prevalence dependent or prevalence-independent.
- ➢ Furthermore, these techniques are used in UPI fraud detection mechanisms, and the results of these algorithms have been compared.

DISADVANTAGES

- ➢ Cases of fraud associated with it are also rising.
- ➢ This algorithm is a heuristic approach used to solve high complexity computational problems.
- ➢ Unfortunately, this popularity also attracts criminals who exploit the complex network environment to commit fraud. Such fraudulent activities not only harm consumers but also impede the healthy growth of the online economy.

PROPOSED SYSTEM

UPI fraud refers to fraudulent activities and scams that take place within the Unified Payments Interface (UPI) system in India with reference to UPI based digital transactions. Fraudsters use various tactics to deceive individuals and exploit vulnerabilities in the UPI ecosystem. Fraudsters often trick you into revealing their UPI PIN or personal information, enabling them to access your bank accounts and carry out fraudulent transactions.

- "Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction.
- A deadlock **detection algorithm** is a technique used by an operating system to identify deadlocks in the system. This algorithm checks the status of processes and resources to determine whether any deadlock has occurred and takes appropriate actions to recover from the deadlock.
- Few steps involving UPI transaction process using a **Hidden Markov Model (HMM)**

ADVANTAGES

- Finding optimal solution for the problem and implicitly generating the result of the fraudulent transaction.
- The main aim is to detect the fraudulent transaction and to develop a method of generating test data.
- The implementation of an efficient fraud detection system is imperative for all UPI issuing companies.

MODULES DESCRIPTION

UPI CREATION

- User downloads the UPI application from the App Store/Banks website.
- User creates his/her profile by entering details like name, virtual id (payment address), password etc.
- User goes to “Add/Link/Manage Bank Account” option and links the bank and account number with the virtual id.

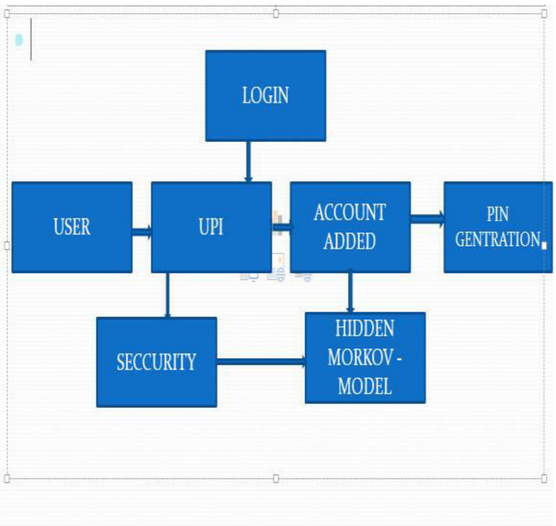
UPI CATEGORY

Unified Payments Interface (UPI) is an instant payment system developed by the National Payments Corporation of India (NPCI), an RBI regulated entity. UPI is built over the IMPS infrastructure and allows you to instantly transfer money between any two parties' bank accounts.

TRANSACTION

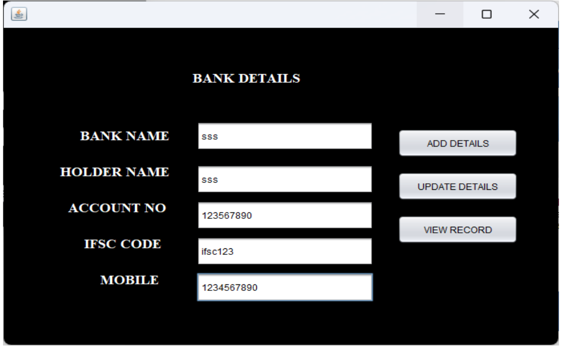
- A transaction involves a monetary exchange for a good or service.
- Transactions can be a little more tricky when it comes to corporate accounting.
- Accrual accounting recognizes a transaction immediately after it is finalized, regardless of when payment is received or made.
- Cash accounting is used mostly by smaller businesses and records a transaction only when money is received or paid out.
- Third-party transactions can often complicate the process.

ARCHITECTURE DIAGRAM



Result Analysis

The threat posed by financial transaction fraud to organizations and individuals has prompted the development of cutting-edge methods for detection and prevention. The use of real-time monitoring systems and Cyber Security algorithms to improve fraud detection and prevention in financial transactions is explored in this research study. The paper addresses the drawbacks of conventional rule-based systems, explains why real-time monitoring and Cyber Security should be used, and describes the goals of the research. To comprehend the current methodologies and pinpoint research gaps, a thorough literature study is done. The suggested approach includes dimensionality reduction, feature engineering, data preparation, and the application of Cyber Security models built into a real-time monitoring system. Results are assessed using performance measures and contrasted with the performance of current systems. Two proactive fraud prevention techniques under investigation are adaptive thresholds and dynamic risk scoring. Considerations for scalability and deployment, including data security and legal compliance, are also covered. The study suggests areas for additional research in this field and helps to design reliable fraud detection systems.



BANK DETAILS

BANK NAME sss

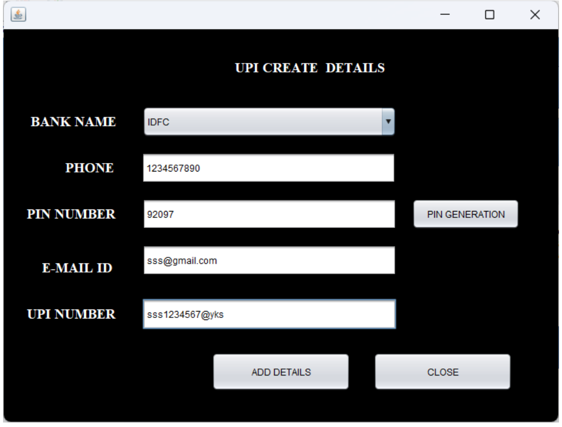
HOLDER NAME sss

ACCOUNT NO 123567890

IFSC CODE ifsc123

MOBILE 1234567890

Fig-1 Bank details



UPI CREATE DETAILS

BANK NAME IDFC

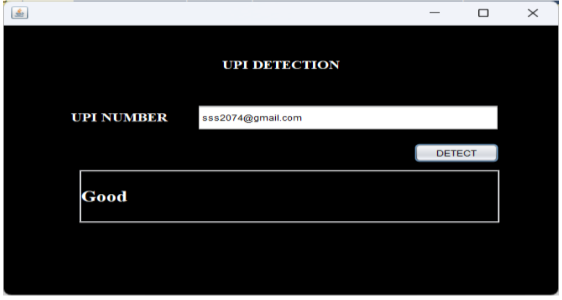
PHONE 1234567890

PIN NUMBER 92097

E-MAIL ID sss@gmail.com

UPI NUMBER sss1234567@yks

Fig-2 UPI Creation

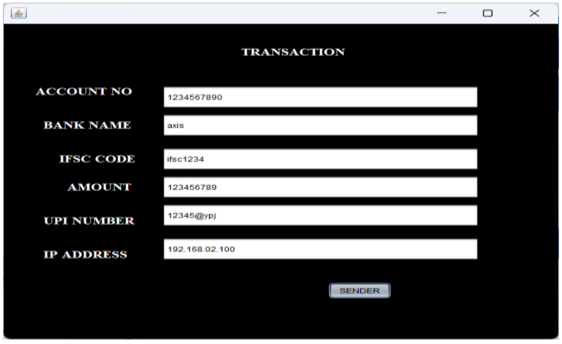


UPI DETECTION

UPI NUMBER sss2074@gmail.com

Good

Fig-3 UPI Detecction


TRANSACTION

ACCOUNT NO 1234567890

BANK NAME axis

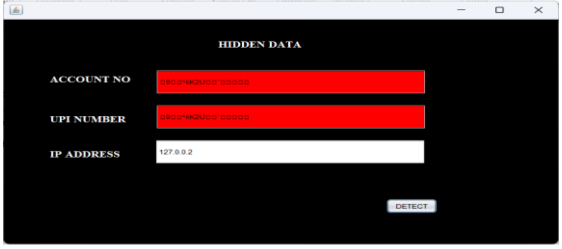
IFSC CODE ifsc1234

AMOUNT 123456789

UPI NUMBER 12345@ypj

IP ADDRESS 192.168.02.100

Fig-**4** Transaction


HIDDEN DATA

ACCOUNT NO □9□□^kK2U□□`□□□□□

UPI NUMBER □9□□^kK2U□□`□□□□□

IP ADDRESS 127.0.0.2

Fig-5 Fraud Detection

IV. CONCLUSION

In this system we developed a novel method for fraud detection, where customers are grouped based on their transactions. We finally observed that involving UPI transaction process using a Hidden Markov Model (HMM) and detection algorithm based upi fraud hidden the upi number and account details that gave better results. Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

REFERENCES

[1] Aditya Oza "Fraud Detection using Machine Learning" - https://github.com/aadityaoza/CS-229- project.

[2] Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omanna, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai. "Online Transactions Fraud Detection using Machine Learning" Volume 5, Issue 6 June 2023, pp: 545-548 www.ijaem.net

[3] M. Valavan and S. Rita "Predictive-Analysis-based Machine Learning Model for Fraud Detection withBoosting Classifiers" Computer Systems Science & Engineerin

[4] Abdulalem Ali 1,,Shukor Abd Razak 1,2,ORCID,Siti Hajar Othman 1ORCID,Taiseer Abdalla Elfadil Eisa 3,Arafat Al-Dhaqm 1,ORCID,Maged Nasser 4ORCID,Tusneem Elhassan 1,Hashim Elshafie 5 andAbdu Saif 6ORCID "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review" https://doi.org/10.3390/app12199637.

[5] PayPal Inc. Quarterly results https://www.paypal.com/stories/us/paypalreports-third-quarter-2018-results

[6] A Model for Rule Based Fraud Detection in Telecommunications - Rajani, Padmavathamma - IJERT – 2012

[7] HTTP Attack detection using n−gram analysis - A. Oza, R.Low, M.Stamp - Computers and Security Journal - September 2014

[8] Scikit learn - machine learning library http://scikit-learn.org

[9] Paysim - Synthetic Financial Datasets for Fraud Detection https://www.kaggle.com/ntnu-testimon/paysim1

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com