JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

UPIGUARD: Secure Your UPI Transactions

[1]Sadhana Singh, [2]Shikhar Raj, [3]Shreya Tyagi
[1]Assistant Professor, [2]B.Tech.*, [3]B.Tech.*
[1,2,3]CSE-AI,
[1,2,3]ABES Institute of Technology, Ghaziabad, India

Abstract: Unified payments interface is a very important element of digital finance. In this paper, we will learn about the UPI and the fraudulent activities related to UPI. The technology used to detect and stop fraud in UPI is known as the UPIGAURD, this technology helps in detecting fraud using machine learning and artificial intelligence. UPI or unified payments interface is a real-time payment system in India that facilitates instant money transfer using mobile, using UPI is beneficial because it helps in money transfer from one bank account to another bank account without any deduction of taxes and charges. Everything that comes with a benefit has its disadvantages, UPI can cause a lot of easements but with this, comes fraud, many fraudulent activities and, incidents have come up regarding UPI suggesting that all of the money in the account is stolen using access to the UPI.

Index Terms **- UPI Fraud, SIM swap fraud, digital finance, security measures and financial transactions.**

I. INTRODUCTION

UPIGaurd is an innovation which will be used to detect and stop fraud against upi using machine learning techniques. Don't compromise your financial security any longer. Stay superior to UPI fraud – because your security matters.
Although there are many key features in UPI such as: -
Seamless transactions, Mobile-centric, Multiple bank accounts, Virtual payment address (VPA), Two-factor authentication, Immediate fund transfer and Merchant payments.
One of the primary challenges we're facing in our project is the scarcity of datasets. Datasets are essentially large sets of examples and information that our system needs to learn and understand patterns related to UPI fraud detection. However, obtaining these datasets is proving to be difficult because banks don't want to share the detailed transaction information of their clients with us.
Banks prioritize the security and privacy of their customers. As a result, they are not willing to provide us with the actual data from their clients' transactions. Imagine trying to teach a computer to recognize different types of animals, but you're only allowed to show pictures of a couple of species. The computer won't have a broad understanding, making it less capable when encountering new, unseen species. Similarly, without a diverse dataset, our system might struggle to identify new patterns or variations of fraud that haven't been seen before.
Solutions for these challenges are: Synthetic Datasets, Data Masking and Anonymization, Simulated Environments, Collaborative Research Agreements, Use Public Datasets, Data Augmentation Techniques, Focus on Feature Engineering, Secure Data-Sharing Protocols, Educational Initiatives and Explore Open Innovation Platforms.

1.1 Fraud Related to UPI

Frauds related to UPI fraud can take various forms, and it's important for users to be aware of the potential risks and practice safe digital financial habits. Here are some common types of UPI frauds: -
Phishing: Fraudsters may send fake emails, messages, or calls posing as some banks or UPI service providers and trick the users.
Fraudulent UPI IDs: Fraudsters create fake UPI IDs and QR code to receive funds.
SIM Swap Fraud: Fraudsters convince the mobile service providers to swap the numbers of its users and gain the control of the messages and use the OTPs to gain access to the bank account.
Malicious app: Users unknowingly download malicious apps that mimic UPI interface.
Remote desktop access: Fraudsters convince victims to install remote desktop applications, allowing them to access the victim's device and conduct unauthorized transactions.

II. LITERATURE SURVEY

Table 2.1: Comparison table of different papers

Author name	Title	Purpose	Summary	Reference number
Deepti Sisodia, Dilip Singh Sisodia	A transfer learning framework towards identifying behavioral changes of fraudulent publishers in pay-per-click model of online advertising for click fraud detection	To contribute to the field of click fraud detection in online advertising by proposing an innovative framework	This paper focuses on identifying behavioral changes in publishers, which can serve as an effective method for detecting fraudulent activity and protecting advertisers from financial losses.	[1]
Yufei Liang, Jiangning Zhang, Shiwei Zhao, Runze Wu, Yong Liu, Shuwen Pan	Omni-Frequency Channel-Selection Representations for Unsupervised Anomaly Detection	To introduce a novel approach for unsupervised anomaly detection, focusing on sensory anomaly detection tasks	It introduces a novel approach to unsupervised anomaly detection using omni-frequency channel-selection representations to capture essential features across different frequency domains, potentially offering a valuable contribution to the field of anomaly detection.	[2]
Guansong Pang, Chunhua Shen , Huidong Jin , Anton van de Hengel	Deep Weakly-supervised Anomaly Detection	To present an innovative and effective approach for weakly-supervised anomaly detection, with a specific focus on detecting both known and unknown anomalies.	The paper demonstrates the effectiveness of weakly-supervised learning principles in training deep neural networks for anomaly detection tasks and highlights potential applications across various domains.	[3]
Todd Zhou and Hong Jiao	Exploration of the Stacking Ensemble Machine Learning Algorithm for Cheating Detection in Large-Scale Assessment	To assess the performance of the stacking ensemble machine learning algorithm in identifying cheating behaviors.	The authors likely present the results of their experiments, showing how well their stacking ensemble method performs in detecting cheating in large-scale assessments compared to individual models or other methods.	[4]
Dr. Alessio Faccia	National Payment Switches and the Power of Cognitive Computing against Fintech Fraud	It provides real-world examples of how cognitive computing is used in NPSs to identify fraudulent transactions and suggests best practices for implementing cognitive computing in fraud detection.	This research highlights the critical role of cognitive computing tools in preventing and detecting financial fraud within National Payment Switches (NPSs), and provides insights for future research in evaluating the success rate, cross-border fraud detection, regulatory compliance, integration with existing systems, privacy and security concerns, and emerging trends in this rapidly evolving field.	[5]
Mallikarjun H, Rishith C, Rakesh S V, Sandeep Kumar K, Vinay Varade Gowda K	E-Banking Fraud Detection System Using Stacking method (On Ensemble Learning)	To address the challenges and ambiguities inherent in online transactions, particularly in the context of e-commerce, stock trading, and various forms of digital payment methods, such as credit cards, debit cards, and UPIs	The paper aims to improve the accuracy and reliability of fraud detection models to safeguard e-banking transactions and mitigate financial risks.	[6]

III. Fraud Detection System

Fraud detection system is a system that uses machine language to search, detect , and try to find the missing errors or abnormalities in the UPI transactions , the UPIGaurd uses fraud detection system to find the missing errors in the large database given by the banks , the banks give out the larger database of their client such as transaction details and the details of the sender / receiver , machine learning studies the dataset and finds the common links or the similarities between frauds or the fraudsters , this helps the machine to understand the similarities between the fraudsters and then identifies the fraudsters using that information , according to these information the machine detects the fraudsters and then tells the users of UPIGaurd to be careful as the opposite party may be fraud . Fig.1 shows the process of fraud detection system.

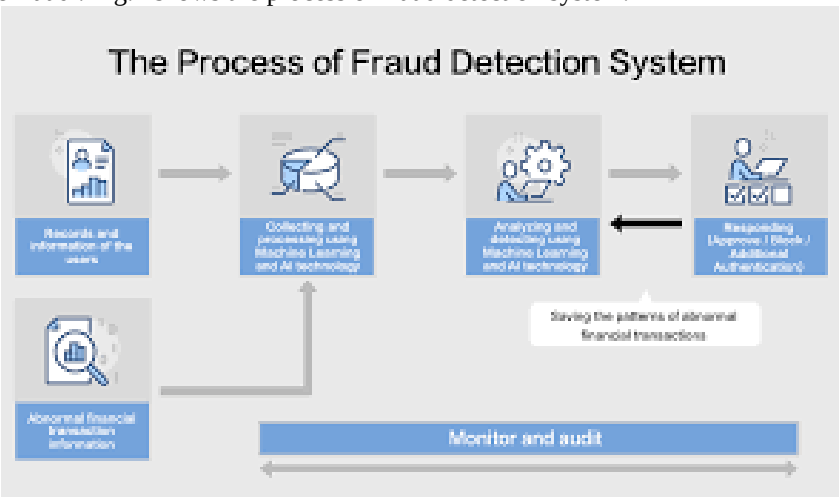

Figure 1. Flow of Fraud Detection System

IV. Conclusion

In today's world, where most of our money dealings happen online, it's crucial to protect those transactions from the always-changing risk of fraud. This project focused on stopping fraud in a specific online payment system called UPI.

As we finish up this project, we're proud of the progress we've made in making digital transactions more secure. Our system is advanced and can tell the difference between real transactions and fake ones really well, showing how dedicated we are to making sure UPI is a trustworthy system.

However, we know that fraudsters are always coming up with new tricks. So, we're saying it's super important to keep working closely with other important groups, like banks, regulators, and cybersecurity experts. By teaming up, we can spot new threats early and make UPI even more resistant to fraud.

As we wrap up this project, we're feeling pretty good about what we've done. We've made a smart system that's really good at telling when a transaction is real and when it's a fake. This shows how serious we are about making sure UPI is a safe and reliable way to handle money online.

But, here's the thing: the bad guys are always coming up with new tricks. So, we're saying it's not enough to just stop them now; we need to keep working together with other important groups, like banks, rule-makers, and computer security experts. If we team up, we can find out about the new tricks early and make UPI even stronger against these bad actions.

To sum it up, this project proves how using data and smart ideas can make online transactions safer. Looking forward, we're committed to making UPI fraud detection even better, so people can use digital money with confidence and peace of mind.

V. Acknowledgment

We really thankful to God, our family members to making this possible.

References

[1] Deepti Sisodia, Dilip Singh Sisodia, "A transfer learning framework towards identifying behavioral changes of fraudulent publishers in pay-per-click model of online advertising for click fraud detection", Expert Systems with Applications ,Volume 232,120922 (2023).

[2] Y. Liang, J. Zhang, S. Zhao, R. Wu, Y. Liu and S. Pan, "Omni-Frequency Channel-Selection Representations for Unsupervised Anomaly Detection," in IEEE Transactions on Image Processing, vol. 32, pp. 4327-4340, 2023.

[3] Guansong Pang, Chunhua Shen, Huidong Jin, Anton van den Hengel,"Deep Weakly-supervised Anomaly Detection", KDD '23: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (2023).

[4] Todd Zhou and Hong Jiao, "Exploration of the Stacking Ensemble Machine Learning Algorithm for Cheating Detection in Large-Scale Assessment", Educational and Psychological Measurement, Volume 83 (2022).

[5] Dr. Alessio Faccia, "National Payment Switches and the Power of Cognitive Computing against Fintech Fraud", *Big Data Cognitive Computing*, *7*(2), 76 (2023).

[6] Mallikarjun H, Rishith C, Rakesh S V, Sandeep Kumar K, Vinay Varade Gowda K,"E-Banking Fraud Detection System Using Stacking method (On Ensemble Learning)", Recent Trends in Androids and IOS Applications,Vol 5, No 3 (2023).