Fortifying Digital Payments: Responding to UPI Frauds by Leveraging AI and Blockchain Technology

Srikrish Santhosh[1], Tanisha Parvatikar[2]
Department of Commerce, St. Xavier's College, Mumbai

***Abstract*—-This report focuses on India's broad digital payment market and illustrates a sharp rise in digital payment's fraud, as shown through a case study. The paper suggests using machine learning and blockchain smart contracts for anomaly detection as cutting-edge security techniques to counteract emerging risks. While blockchain smart contracts offer a decentralized and unchangeable base, anomaly detection examines user behavior to strengthen the digital payment system. In addition to addressing existing gaps in security, these suggested laws also support a dialogue that places a premium on accessibility and trust, establishing the framework for India's safe and ongoing use of electronic payment systems.**

***Index Terms*—-Anomaly Detection, Blockchain Smart Contracts, Digital payments, Machine learning.**

I. INTRODUCTION

Digital payments have become an omnipresent reality today, as India leads the global race [1] in the adoption of electronic payment systems, evident in the 45% CAGR in digital payments between FY 2017-18 and FY 2022-23 [2].

However, the rate of frauds has seemed to increase steadfastly with the rapid growth in digital payments, particularly with UPI having the highest share in terms of volume, accounting for 55% of the total number of digital payment frauds in 2022 (PwC India, 2022). The year 2022 saw 95,000 UPI frauds, recording an increase of 11,000 from the year prior [3]. Phishing, pharming, skimming, account takeover fraud and automated clearing house fraud are some of the commonly identified fraudulent activities deployed to rob end-users.

The safeguarding of digital financial transactions has become critical, necessitating creative and flexible approaches to maintain the integrity of these systems.

In light of this, this study examines the difficulties brought about by the rising fraud rate in India's digital payment market. It aims to comprehend the dynamics of this dynamic ecosystem, where a complex landscape is created by the meeting point of security flaws and technology breakthroughs. The paper seeks to further the existing discussion on bolstering the security of digital payments and guaranteeing a reliable financial environment for all users by exploring the intricacies of this digital transition.

II. LITERATURE REVIEW

Digital payments frauds have doubled in the FY2023. Information from the Reserve Bank of India's (RBI) FY23 annual report revealed that while the total value of frauds reported by Indian banks decreased by half from 59,819 crore in FY22 to 30,252 crore in FY23, the volume of digital frauds committed using cards and internet-based payment methods nearly doubled in the previous financial year.

While there were 3,596 recorded frauds in FY22 totaling 155 crore that involved cards and online banking services, the number almost quadrupled to 6,659 digital frauds totaling 276 crore in FY23. Nonetheless, there were delays in the detection of fraud and the consequent lag in reporting by lenders, with 94.5% of the frauds recorded in FY23 by value occurring in prior financial years [4].

To further understand the implications, it is necessary to comprehend the significant literature in addition to the regulatories and their effects. This review of the literature attempts to offer a thorough examination of academic publications, research studies, and scholarly works that further helps our research.

With an emphasis on account-based and token-based techniques, the study by [5] investigates the growth of fraud in electronic payment systems. Using sophisticated security standards, regulations, EMV Level 2, and intelligent technologies, it places a strong emphasis on proactive fraud prevention and detection. However, there may not be any practical examples or recommendations on how to use security protocols and intelligence tools in the study.

With a proposal for the gathering and application of fraud data, the [6] tackles the issues of digital payment fraud in the Indian banking sector. A five-level process paradigm is introduced, with an emphasis on proactive interventions. The study does not, however, specifically address the shortcomings of the suggested method or advocate for field testing to determine its efficacy.

Malware and trojans are cited in the study report [7] on e-banking scams as international dangers. It looks at 51 risks and 42 preventative measures. While it helps to understand the security of e-banking, additional real-world examples and real-world problems are required.

The study [8] explores the difficulties associated with e-payments and offers fixes for security, corporate involvement, and less dependency on conventional techniques. Future developments are examined, with a focus on mobile commerce. Narrow focus, data currency issues, and gaps in cultural and regulatory considerations are some of the limitations.

The research study [9] identifies the security risks associated with electronic payment systems and recognizes "TSL" and "SET" as cutting-edge security solutions to protect digital payments. Nevertheless, given the amount of fraud occurring today, these security measures are antiquated.
This study specifically addresses the need for real-world application in the field of digital payment security, which is in response to the shortcomings noted in the body of previous research. The research attempts to improve the performance and relevance of suggested security policies by offering case study and addressing practical issues.

III. METHODOLOGY

A purposive sampling method was employed to select a representative case within the digital payments ecosystem. The chosen case study involved a detailed step-by-step plan deployed to scam its victims.

The selection of the UPI fraud case study is driven by its contemporary relevance and practical insights into challenges faced by digital payment users. The complex nature of the UPI fraud provides a rich subject for detailed exploration and comprehensive solution proposals. The tangible impact on users underscores the urgency of addressing such incidents. Incorporating insights from experts and service providers enriches the analysis, providing a thorough assessment of UPI fraud implications. Beyond serving as a cautionary tale, this case study aligns with the proposed policies, offering a pragmatic basis for evaluating effectiveness and contributing to the discourse on digital payment security.

IV. CASE STUDY

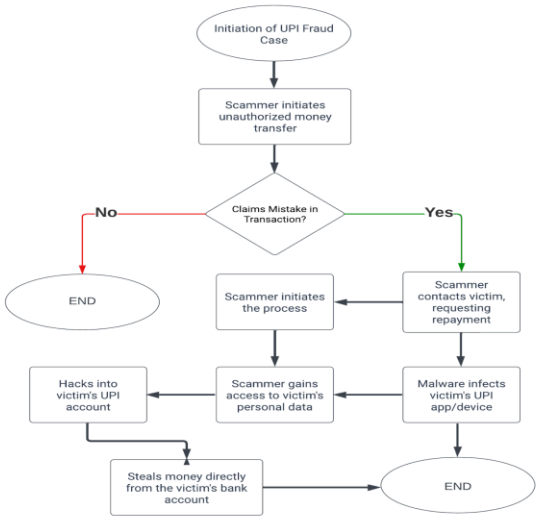
Scammers use "payment mistake" strategies in a UPI fraud case, robbing 81 victims in Mumbai of nearly Rs 1 crore. The scam is sending money using UPI applications, such as Google Pay, then getting victims to reimburse the money by saying there was a mistake. Scammers use malware to breach victims' UPI accounts after they have been reimbursed, taking money straight out of their bank accounts.

The UPI fraud presents a challenge to current anti-virus solutions due to its intricate combination of malware phishing and human engineering. Expert on cybercrime Pavan Duggal highlights the shortcomings of the anti-malware software available today and advises users of UPI to exercise caution. He suggests that victims tell their bank of the problem and tell callers who claim there was a transaction error to pick up the money from the closest police station [10].

Although the UPI system in the aforementioned scenario is safe and secure, it is feasible for hackers to construct and distribute phony URLs that appear to provide the ability to "request money" [10]. This link will prompt the user to scan a code or provide the UPI pin as soon as clicked. Malware connected to these

links can then take advantage of the user's private data [11].

Flow chart illustrating the scam's operation:



This case study on UPI fraud provides valuable insights that clarify the complex issues encountered by digital payment users and reinforce the justification for enacting the suggested regulations. The policies recommended in this paper are shown to be strong solutions that are suited to handle and reduce the risks that have been discovered by looking at the practical ramifications and vulnerabilities that the case study reveals. The case study on UPI fraud provides strong confirmation, highlighting the usefulness and efficiency of our suggested actions in boosting the security of digital payments.

V. PROPOSED POLICIES

The following proposed policies address the shortcomings of existing digital payment security policies and bridge the gap between user preparedness and fraud intelligence.

Anomaly Detection Through Machine Learning:

Incorporate machine learning algorithms for anomaly detection [12] into digital payment systems. These algorithms can analyze large datasets of user behavior, transaction history, and other relevant variables to establish a baseline of normal activity. Deviations from this baseline, which may indicate fraudulent behavior, can trigger alerts or additional security measures. Their financial activities' capability, transaction caps etc. can be curtailed on the basis of their "anomaly score", which helps label a bank account/e-money user as *potentially fraudulent*.

Such a database shall be managed at the governmental level, leveraging the country's IT resources to maintain a database of user behavior that updates in real-time. It should be connected to banks, users and the monetary authority alike to signal to them an anomaly occurring beyond set parameters of danger.

Blockchain Smart Contracts:

Blockchain can be defined as a large distributed database, in which it is possible to record transactions of all kinds between the parties, directly, securely and in real time, without the need for intermediaries and with total traceability. The key properties of integrity, resilience, and transparency [13] make blockchain a lucrative policy or protection tool. While blockchain has several use-cases, an effective one in the context of securing digital payments is the use of smart contracts.

Smart contracts are programs stored in a blockchain that are executed when a predetermined condition is satisfied [14]. They execute the terms of a contractual agreement using computerized transaction protocols [15].

This paper proposes an amalgamation of the anomaly detection algorithm (stated earlier) and smart contracts to automate the security of digital payments.

A digital payment app running on blockchain technology can use smart contracts to assess if a UPI account is safe to transact with based on their banking history. The predetermined conditions that bind this transaction, within a smart contract, will be that the opposite party has 'non-deviant' banking behavior or an acceptably low anomaly score in an appropriately chosen period of time in the past. A payment initiated against a *potentially fraudulent* UPI account, as a result, will simply not proceed because the predetermined condition binding the transaction is unfulfilled.

It is noteworthy that there is minimal risk of hacking a smart contract. Once a smart contract is created and stored in a blockchain, it is immutable, and thus cannot be modified [16].

Thus, such a blockchain technology can be mandated to form the basis of digital payment applications created by e-money issuers (including banks). Importantly, the decentralized nature of blockchain technology should not abate the monetary authority's responsibility to audit the proper functioning and maintenance of the blockchain technology periodically.

VI. CONCLUSION

In a nutshell the exponential rise in digital payments in India has transformed financial transactions, but as the case study shows, this expansion is accompanied with a worrisome rise in UPI fraud.

The suggested policies provide a progressive method of addressing these issues. When combined with blockchain smart contract integration, anomaly detection using machine learning—which examines user behavior and transaction patterns—offers a viable path toward improving the security of digital payments. These steps attempt to automate the identification of fraudulent activity, develop a decentralized and immutable framework, and eventually enhance the resilience of the digital payment ecosystem.

The necessity of an inclusive policy implementation process and a strong IT infrastructure are two examples of potential constraints that must be acknowledged. In addition to filling in existing security weaknesses, the suggested solutions further the ongoing discussion about creating a safe and user-friendly digital financial ecosystem. In India's changing financial environment, maintaining the security of digital transactions is not just a question of technology development but also of fostering a culture of trust and guaranteeing the long-term uptake of electronic payment systems.

VII. DISCUSSION

Acknowledging the limitations of the current study, such as the specificity of the case study, and its large scale making it a one-off incident, opens avenues for future research.

Another potential limitation is that solutions such as 'anomaly detection' and 'leveraging smart contracts' require sturdy IT infrastructure to develop and maintain; they may place considerable stress on the scarce IT resources available in the country.

The scope of future research includes the need for proposed policies and protection tools to be filtered through economic and social lenses too. The tools prescribed above should be made inclusive and easily accessible to all, research for which must ensue in order to lead to its stealthy implementation in the near future.

REFERENCES

[1] India's digital payments in 2022 more than US, UK, Germany, France economies combined: Ashwini Vaishnaw at WEF. (2023, January 20). *Mint.* https://www.livemint.com/news/india/indias-digital-payments-in-2022-more-than-us-uk-germany-france-economies-combined-ashwini-vaishnaw-at-wef-11674200318147.html

[2] Press Information Bureau. *Total digital payment transactions volume increases from 2,071 crore in FY 2017-18 to 13,462 crore in FY 2022-23 at a CAGR of 45 per cent: MoS Finance.* (2023, December 19). https://pib.gov.in/PressReleseDetail.aspx?PRID=1988370

[3] Over 95,000 UPI fraud cases reported in 2022-23: Centre in Parliament. (2023, March 23). *Hindustan Times.* https://www.hindustantimes.com/india-news/over-95-000-upi-fraud-cases-reported-in-2022-23-centre-in-parliament-101679541121388.html

[4] Financial Express. (2023, 5th June). Banking, finance, banks: Digital payments frauds nearly double in FY23. The Financial Express. [URL: https://www.financialexpress.com/business/banking-finance-banks-digital-payments-frauds-nearly-double-in-fy23-3113522/]

[5] Simić, D. (2005). Reducing Fraud in Electronic Payment Systems. *Proceedings of the 7th Balkan Conference on Operational Research (BACOR '05)*, Constanta, Romania, May 2005.

[6] Priya, N., Ahmed, J., & Alam, M. A. (2020). Digital Payments: A Scheme for Fraud Data Collection and Use in Indian Banking Sector. *International Journal of Innovations in Management, Science and Engineering (IJIMSE)*

[7] Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques. Linguistica Antverpiensia, 2021 Issue-2.

[8] Raja, J., Senthil Velmurgan, M., & Seetharaman, A. E-payments: Problems and Prospects. *Journal of Internet Banking and Commerce*.

[9] Kharb, Latika & Shubham, & Chahal, Deepak. (2018). "Security for Digital Payments: An Update," *Int. J. Sc. Res. in Network Security and Communication.*

[10] Kumar, R., Kishore, S., Lu, S., & Prakash, (2020). A. Security Analysis of Unified Payments Interface and Payment Apps in India. *29th USENIX Security Symposium* https://www.usenix.org/system/files/sec20-kumar.pdf

[11] Divya Bhati. "Scammers Steal Rs 1 Crore from 81 Users in Mumbai While Making UPI Payment: How to Stay Safe." India Today, 27 March 2023, https://www.indiatoday.in/technology/news/story/scammers-steal-rs-1-crore-from-81-users-in-mumbai-while-making-upi-payment-how-to-stay-safe-2351854-2023-03-27?onetap=true.

[12] Hilal, W., Gadsden, S., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Journal of Expert Systems With Applications*. https://doi.org/10.1016/j.eswa.2021.116429

[13] Blockchain Characteristics and Consensus in Modern Business Processes. (2018). *Journal of Industrial Informatic Integration 1*. https://www.researchgate.net/profile/Wattana-Viriyasitavat/publication/326680277_Blockchain_Characteristics_and_Consensus_in_Modern_Business_Processes/links/5ee9c67a299bf1faac5c8a37/Blockchain-Characteristics-and-Consensus-in-Modern-Business-Processes.pdf

[14] "ETSI executive briefing - mobile edge computing (mec) initiative."

[15] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, & F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266–2277, 2019.

[16] H.-N. Dai, Z. Zheng, & Y. Zhang, "Blockchain for Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, 2019.