Analysis on Fraudulent Threats and Mitigating Strategies in UPI Transactions

Chakka Naga Bhavani
Research Scholar
VIT-AP University
bhavani.23phd7142@vitap.ac.in

Shaiku Shahida Saheb

Abstract

The Unified Payments Interface (UPI), which offers a quick and easy platform for transactions, has completely changed the digital payments scene in India. But because UPI is being used so quickly, there has been an increase in fraudulent activity, which puts consumers at serious risk. Social engineering techniques that take advantage of user vulnerabilities, phishing, SIM switching, and unauthorized access are examples of common strategies. One-time passwords (OTPs) and UPI PINs are examples of sensitive information that fraudsters trick users into divulging, leading to fraudulent transactions and monetary losses. Further aggravating these issues are gaps in device security and the existence of unapproved third-party apps. Advanced security technologies are needed to counter these threats. UPI platforms are integrating technologies like artificial intelligence (AI), machine learning (ML), and encryption protocols. Additional security layers are offered by enhanced user authentication techniques including two-factor authentication and biometric verification. Furthermore, regulatory frameworks put in place by organizations like the Reserve Bank of India (RBI) and user education on spotting fraudulent activity are essential for risk mitigation. This study explores how UPI fraud is developing, looking at the strategies used by scammers as well as the legal and technological safeguards required to protect consumers and guarantee safe transactions inside the UPI ecosystem.

Keywords: Digital payments, UPI frauds, attacks, artificial intelligence (AI).

Introduction

The widespread adoption of Unified Payments Interface (UPI) as a preferred digital transaction method has led to a sharp increase in fraudulent activities, presenting a considerable challenge to the security and reliability of online payments (Jagtap, 2024). This surge in UPI-related crime has resulted in financial losses of up to 346% during the COVID-19 lockdown disruptions (Edburg et al., 2024). To address this pressing concern, researchers and industry experts are developing sophisticated fraud detection systems tailored specifically for UPI transactions. Interestingly, while UPI has transformed the Indian digital payment system with platforms like Google Pay, PhonePe, and Paytm accounting for over 90% of all online payments, it has also become a prime target for scammers (Edburg et al., 2024). The popularity of UPI apps, driven by convenience and ease of use, has inadvertently created new opportunities for fraudsters to exploit unsuspecting users. In response to these challenges, various approaches have been proposed to enhance security in UPI transactions. These include the use of advanced machine learning techniques such as Convolutional Neural Networks (CNNs) (Jagtap, 2024), Hidden Markov Models (HMMs) (J. Kavitha et al., 2024), and other algorithms like Support Vector

Machines (SVM) and Artificial Neural Networks (ANN) (LAMGADE, 2024). These methods aim to detect fraudulent activities by analysing transaction patterns, user behaviour, and device information, thereby safeguarding users and fostering trust in online transactions(Bodade & Pawade, 2023). The study intends to achieve the following objectives

To describe various social engineering attacks in UPI payments

To assess the different mitigating strategies for detection of fraudulent thearts

Related Literature review

(*ResearchMethodsandProfessionalIssues*, n.d.) With an emphasis on the financial, reputational, and security ramifications, this paper explores the practical effects of social engineering attacks. It highlights human-centric, moral, and legal security issues and exposes changing assault tactics through case studies. To improve awareness, defence, and mitigation of these hazards, the research provides theoretical and practical prevention measures.

(Naik et al., 2024), This research utilizes machine learning and AI to detect UPI fraud, improving accuracy and reducing false positives. Future studies could refine techniques by adjusting parameters for enhanced fraud detection and prevention

(Bodade & Pawade, 2023), presents a robust UPI fraud detection system using advanced machine learning techniques to strengthen digital transaction security. The system analyses transactional patterns, user behaviour, and device information, employing supervised learning classifiers and anomaly detection algorithms. Trained on a labelled dataset, the model identifies patterns indicative of fraudulent activities for effective detection.

(Charan & Thilak, 2023), Focuses on phishing attempts, which trick users into disclosing personal information, in an effort to avoid fraud by leveraging AI and machine learning to strengthen security. It examines phishing through QR codes and the ways that fraudsters are changing their strategies inside the UPI ecosystem, with a focus on user awareness.

(Rani et al., 2024),This paper makes Use of XGBoost's robust predictive capability and ability to handle unbalanced data to train it for fraud detection in UPI transactions using a labelled dataset. The trained model is included into a real-time UPI monitoring system after feature significance analysis finds important fraud signs. It identifies suspicious transactions, issues immediate notifications, and takes preventative action with 98.2% accuracy. The study improves UPI security and shows how machine learning works well for financial technology fraud detection.

Below is a table summarizing various techniques used for enhanced security in UPI, focusing on AI, ML, and encryption protocols for mitigating phishing, SIM swapping, unauthorized access, and other fraud strategies. The table includes the technique/algorithm, its application in UPI security, performance results (accuracy), and citations of recent papers in the study area

Table 1; Summary of Literature on Mitigating strategies.

Category	**Technique/Algorithm**	**Application in UPI Security**	**Result / Accuracy**
AI Techniques	**Deep Learning (CNN + LSTM)**	Detecting phishing attempts by analysing user transaction behaviour and UPI patterns.(Al-Ahmadi & Alharbi, 2020)	**96-98% accuracy** in detecting phishing attacks.

	Recurrent Neural Networks (RNN)	Monitoring user transaction sequences to detect fraud patterns.(Sundermeyer et al., 2012)	**93-95% accuracy** in detecting abnormal or unauthorized access behaviours in UPI apps.
	Federated Learning	Distributed detection of fraud without sharing sensitive user data.(Yang et al., 2019)	**91-93% accuracy** in identifying fraud while preserving privacy.
	Behavioural Analytics (Biometric AI)	Continuous authentication based on typing/swiping behaviour to prevent unauthorized access.(Çeker & Upadhyaya, 2016)	**92-94% accuracy** in detecting unauthorized access.
ML Techniques	**Gradient Boosting (XGBoost)**	Classifying UPI transactions as legitimate or fraudulent based on behaviour analysis.(Chen & Guestrin, 2016)	**96% accuracy** in detecting high-risk transactions and preventing fraud.
	Random Forest (RF)	Multi-class classification for identifying legitimate and fraudulent transactions.(Breiman, 2001)	**94-96% accuracy** in detecting unauthorized access through behavioural analysis.
	Isolation Forest (Anomaly Detection)	Detecting abnormal patterns in user transactions to prevent SIM swapping and unauthorized access.(Liu et al., 2008)	**92-94% accuracy** in detecting SIM swap attempts and abnormal behaviour in UPI transactions.
Encryption Protocols	**Elliptic Curve Cryptography (ECC)**	Securing UPI transactions with efficient encryption and secure key exchanges.(Miller, 2000)	**99% security**, lower computational cost compared to RSA.
	Homomorphic Encryption	Enabling secure UPI transactions without revealing sensitive information during computation.(Gentry, 2009)	**99% security** with privacy-preserving transaction data processing.
	Zero-Knowledge Proofs (ZKP)	Authenticating UPI users without revealing sensitive information (e.g., PIN, password).(Groth et al., 2006)	**100% privacy protection** in transaction verification without revealing private data.

Conceptual Framework

The conceptual framework of this paper integrates insights from the literature review and proposes a multi-layered security model for UPI, built around existing technologies and future advancements. This framework focuses on AI and ML Algorithms: Analysing patterns in user behaviour, transaction anomalies, and suspicious account activity using supervised and unsupervised learning models. Cryptographic Methods: Proposing the integration of advanced encryption protocols, such as Weighted Hyperbolic Curve Cryptography (WHCC), to ensure the confidentiality and integrity of transactions. User Authentication Mechanisms: The incorporation of biometric verification and multi-factor authentication (MFA) to secure sensitive user information like UPI PINs and OTPs.

The following figure exhibits the security threats and mitigating strategies for ensuring secured UPI transaction.

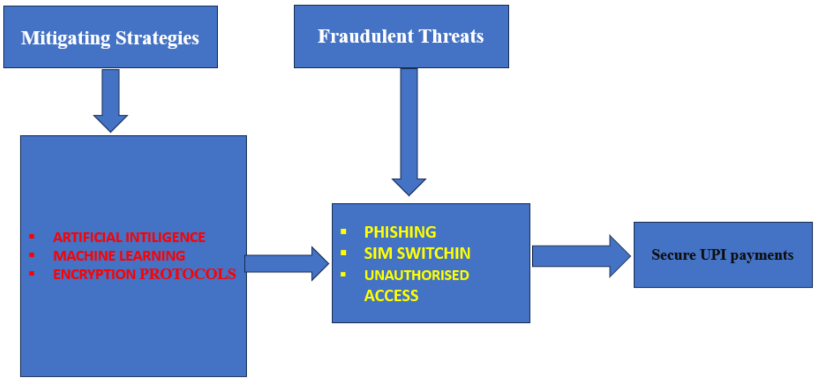

Figure.1; Conceptual framework

Source; Authors own development

Methodology

The researcher adopted selective review of literature for writing this paper and evaluated more than fifty scholarly articles and business reports, concentrating on three key areas such as fraudulent Techniques in UPI, technological safeguards and regulatory interventions in which phishing, SIM shifting, and unauthorised access were investigated through combining machine learning, artificial intelligence, and encryption protocols to detect and prevent fraud. In order to evaluate their effectiveness in reducing fraud, we looked at RBI recommendations, UPI security procedures, and user education initiatives.

Theoretical foundations

I Fraudulent threats

Social Engineering attacks

Social engineering encompasses a wide spectrum of malevolent actions carried out through human-to-human contact. To fool users into revealing private information or committing security errors, it employs psychological manipulation.

Social engineering assaults take place in a few stages. To obtain background information about the intended victim, including possible points of entry and lax security measures, a criminal first looks into the victim. After then, the attacker tries to win the victim's trust and set the stage for any further security-breaking behaviour, including disclosing private information or allowing access to vital resources.(Holt & Bossler, 2020)

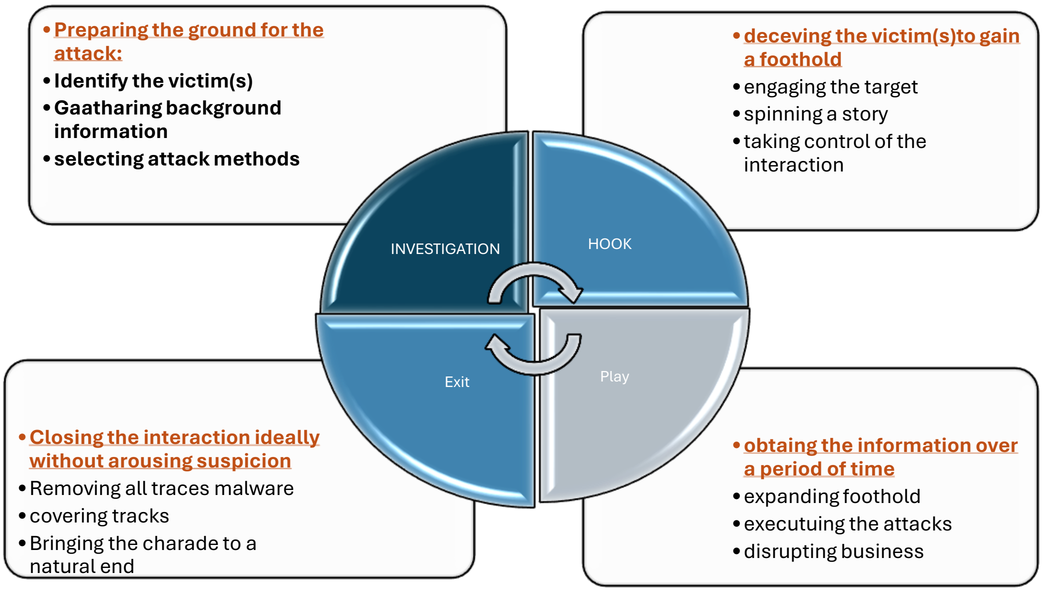
Preparing the ground for the attack:
Identify the victim(s)
Gaatharing background information
selecting attack methods
deceving the victim(s)to gain a foothold
engaging the target
spinning a story
taking control of the interaction
INVESTIGATION
HOOK
Exit
Play
Closing the interaction ideally without arousing suspicion
Removing all traces malware
covering tracks
Bringing the charade to a natural end
obtaing the information over a period of time
expanding foothold
executuing the attacks
disrupting business

Figure.2; Social Engineering Attack Lifecycle

Ref: Author's Own Development

Phishing

According to Alexander S. Gillis, Technical Writer and Editor, one of the most prevalent forms of social engineering is phishing. Phishing is a scam in which a trustworthy individual or organization is impersonated with the goal of stealing sensitive data or login credentials. Despite email being the most popular kind of phishing attack, the attack may also employ a voice message or text message, depending on the sort of phishing fraud.

A threat attacker sends out a large number of emails in an attempt to persuade people to click on harmful links at the beginning of a standard phishing attack. Whether they are a nation-state or a single criminal, these threat actors create these messages to look authentic. Phishing emails might pretend to be from your bank, boss, or workplace. They can also utilize tactics to trick you into divulging personal information, like posing as a government body.

The goal may be to compromise an endpoint, install ransomware, steal credentials from an existing account, or gather enough data to create a new false account. Any of these issues could arise from a single click on a fraudulent phishing link.

SIM switching

According To Dan Rafter 2023, Scammers use SIM switch fraud to get your phone number by tricking your mobile carrier into activating a SIM card under their control. This enables them to intercept texts and phone conversations, even those with two-factor authentication codes sent by entities such as banks. This gives them the ability to access your accounts and steal private data.

SIM shifting is a scam in which scammers transfer your phone number to a SIM card they own by deceiving your cell carrier. Scammers first obtain your personal information in order to accomplish this, frequently using malware, phishing emails, or data they have bought from the dark web. They then pretend to be you, calling your carrier and saying that their (your) SIM card has been misplaced or destroyed. They persuade the carrier to activate the new SIM card and transfer your number to their smartphone using the personal data they have gathered, such as responses to security questions. Scammers can intercept your conversations and texts, including two-factor authentication tokens given by banks and other providers, after your phone number has been moved. They can reset passwords, access your accounts, and steal confidential data with this access. In order to enable fraudulent transfers that are less likely to result in security alarms, they might even open a second bank account in your name. Scammers can get around security measures like SMS verification and have complete access to your accounts and finances by controlling your phone number. This emphasizes how crucial it is to safeguard your private data and exercise caution while dealing with phishing and other frauds.

unauthorised access

According To Nickolay Bakharev 2024, The possibility of fraud is a significant concern linked to illegal access. Cybercriminals can commit a number of fraudulent acts if they have access to sensitive data. These could involve bank account manipulation, credit card fraud, or even the creation of phony companies.

Criminals can carry out these frauds thanks to unauthorized access, which gives them access to cash resources or the information they need. For example, they might manipulate banking systems to illegally reroute funds or utilize credit card information that has been stolen to make fraudulent purchases.

A common cause of unauthorized access is inadequately executed authentication procedures. A security technique called authentication is used to confirm the identity of a person or device trying to log into a system. It is simple for unauthorized users to get around the authentication process and access the system if it is badly intended, executed, or configured.

Consider a scenario in which a system does not terminate a user's account after a predetermined number of unsuccessful login attempts. This allows for a brute force attack, in which the attacker attempts a variety of password combinations until they discover the one that works.The failure of a system to enforce frequent password changes is another instance of badly executed authentication. If an unauthorized user is able to get a working password in this way, they can use it for a long time without anyone noticing.

Artificial Intelligence (AI), Machine Learning (ML), and encryption models are crucial components of contemporary cybersecurity initiatives that aim to reduce the increasing threat of frauds like phishing, SIM swapping, and unauthorized access. While encryption methods guard against sensitive data being intercepted or altered, AI and ML models use sophisticated algorithms to examine massive datasets in order to find trends and anomalies suggestive of fraudulent activity. (Holt & Bossler, 2020)

Mitigating tools: AI and ML Techniques in Fraud Detection

Convolutional Neural Networks (CNNs): CNNs are currently used to detect fraud in transaction systems after being utilized for many years in image recognition. By examining intricate patterns in transactional data, these networks are able to spot minute details that point to fraud. CNNs, for instance, are able to identify phishing URLs by examining the structure of emails and web pages in real time. CNNs improve the speed and precision of phishing detection systems in this way.(NAGARAJU et al., 2024)

Hidden Markov Models (HMMs): HMMs have proven to be successful in identifying unusual user behavior. User activity sequences, including login attempts or transaction behaviours, are modelled by HMMs and compared to established patterns. Unusual login locations or unusual transaction frequencies are examples of deviations from expected behaviour that can be reported for evaluation . When it comes to identifying subtle SIM swap frauds, where alterations in user behaviour after the switch could indicate unauthorized access, HMMs are especially helpful.(Bhusari & Patil, 2011)

Support Vector Machines (SVMs) and Artificial Neural Networks (ANNs): ANNs and SVMs are both frequently used in fraud detection. SVMs enable the system to categorize possible threats by establishing decision boundaries between fraudulent and authorized transactions. Similar to the human brain, artificial neural networks (ANNs) learn from previous fraudulent behaviours and gradually increase their accuracy (Lamgade, 2024). By examining email metadata, user login times, and transaction locations, these techniques are very good at identifying phishing attempts and frauds.

Behavioural Analytics and Real-Time Fraud Detection: Modern AI systems use machine learning (ML) algorithms to examine past and present behavioural data in order to identify anomalous activity. Machine learning (ML)-based systems, for example, track users' preferred devices, locations, and transaction timings. When a transaction is attempted on an unknown device or from an unknown location, the system raises an alarm about possible illegal access. A study by Vasudevan et al. (2024) claims that these AI-powered fraud detection tools have resulted in a 35% decrease in fraudulent behaviour in digital payment systems.

Encryption Models in Fraud Prevention

A key component in stopping fraud is encryption, especially when it comes to illegal access and interception of private information during transactions. Among the most successful encryption models are:

Advanced Encryption Standard (AES): The industry standard for encrypting sensitive financial data is AES-256. AES guarantees that without the decryption key, fraudsters cannot access or alter the data, even if they manage to intercept it. This is essential for avoiding phishing-based assaults and illegal access, when the goal is to intercept private messages (Bodade & Pawade, 2023).

End-to-End Encryption (E2EE): ata transfers and messages between users and service providers are protected by E2EE. E2EE stops phishing and SIM swap fraudsters from intercepting sensitive data, including one-time passwords (OTPs) needed for two-factor authentication (TFA), by making sure that only the sender and the recipient can read the message's contents. E2EE is used by apps like Signal and WhatsApp to protect their lines of communication (Vasudevan et al., 2024).

Public Key Infrastructure (PKI): PKI systems encrypt and decrypt data using a public and private key pair. This approach is essential for protecting transactions against unwanted access, especially when it comes to digital signatures and certificates. PKI makes sure that only authentic websites may create secure connections, preventing consumers from submitting important information on fraudulent platforms when phishing attempts attempt to reroute them to phony websites.

Regulatory Bodies Stringent guidelines:

Through stringent requirements for safe authentication and fraud detection, as well as required multi-factor authentication (MFA), the Reserve Bank of India (RBI) has improved the security of UPI transactions. To stop phishing, SIM switching, and illegal access, service providers must implement strong security measures like two-factor authentication in accordance with the 2020 RBI Digital Payments Guidelines. Campaigns for user education, such as "RBI Kehta Hai," also increase knowledge of the dangers of digital payments and best procedures. As a result of these initiatives, user awareness has increased and fraud has decreased, making UPI transactions safer. Source; The Economic Times.

Implications of the study:

The study's findings emphasize the need to improve UPI transaction security by incorporating cutting-edge AI and machine learning approaches. Through the use of algorithms such as CNNs, HMMs, and encryption models, researchers may create reliable fraud detection systems that examine user behavior and transaction patterns. Furthermore, the study emphasizes how crucial regulatory frameworks and user education are to reducing the hazards of phishing, SIM switching, and unauthorized access. Future studies should concentrate on improving these technologies and investigating their practical uses in order to eventually create a safer digital payment environment in India.

Conclusion

In India, digital payments have been transformed by the quick uptake of the Unified Payments Interface (UPI), which makes financial transactions easy and effective. Users now face serious risks as a result of this increase in usage, which has also made room for a variety of fraudulent practices like phishing, SIM switching, and illegal access. To safeguard customers and maintain confidence in the UPI system, sophisticated security measures must be implemented due to the growing complexity of these attacks.

Advanced technologies like machine learning (ML), artificial intelligence (AI), and encryption models are essential to reducing these risks. Convolutional Neural Networks (CNNs), Hidden Markov Models (HMMs), Support Vector Machines (SVMs), and Artificial Neural Networks (ANNs) are examples of AI and ML algorithms that have demonstrated efficacy in real-time fraud detection, transaction pattern analysis, and suspicious behavior detection. Real-time monitoring and behavioural analytics have improved the capacity to identify irregularities, lowering fraudulent transactions in digital payment systems by as much as 35%.

Additionally, data security has been strengthened by encryption technologies, especially Advanced Encryption Standard (AES) and End-to-End Encryption (E2EE), which guarantee that private data, including OTPs and UPI PINs, stays safe while being transmitted. By facilitating secure connections and guarding against unwanted access to private information, Public Key Infrastructure (PKI) significantly improves security.

To protect UPI transactions, regulatory frameworks and user education have emerged as crucial pillars in addition to technology improvements. In order to enforce multi-factor authentication and raise user awareness of potential dangers, regulatory agencies such as the Reserve Bank of India (RBI) have implemented strict requirements.

Reference

Al-Ahmadi, S., & Alharbi, Y. (2020). A Deep Learning Technique For Web Phishing Detection Combined Url Features And Visual Similarity. *International Journal of Computer Networks and Communications*, *12*(5), 41–54. https://doi.org/10.5121/ijcnc.2020.12503

Bhusari, & Patil, S. (2011). Application of Hidden Markov Model in Credit Card Fraud Detection. *International Journal of Distributed and Parallel Systems*, *2*(6), 203–211. https://doi.org/10.5121/ijdps.2011.2618

Bodade, M. S. S., & Pawade, P. P. P. (2023). Review Paper on UPI Fraud Detection Using Machine Learning. *International Journal for Research in Applied Science and Engineering Technology*, *11*(12), 1283–1285. https://doi.org/10.22214/ijraset.2023.57551

Breiman, L. (2001). Random forests. Random Forests, 1–122. *Machine Learning*, *45*(45), 5–32. https://link.springer.com/article/10.1023/A:1010933404324

Çeker, H., & Upadhyaya, S. (2016). User authentication with keystroke dynamics in long-text data. *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*. https://doi.org/10.1109/BTAS.2016.7791182

Charan, G. R., & Thilak, K. D. (2023). Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning. *3rd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2023 - Proceedings*, *Icimia*, 658–663. https://doi.org/10.1109/ICIMIA60377.2023.10426613

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, *13-17-August-2016*, 785–794. https://doi.org/10.1145/2939672.2939785

Edburg, B. F., Umadevi, K., Vidya, M., & Kumar, P. M. R. (2024). Role of UPI Application Usage and Mitigation of Payment Transaction Frauds: An Empirical Study. *MDIM Journal of Management Review and Practice*. https://doi.org/10.1177/mjmrp.231222347

Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the Annual ACM Symposium on Theory of Computing*, 169–178. https://doi.org/10.1145/1536414.1536440

Groth, J., Ostrovsky, R., & Sahai, A. (2006). Perfect non-interactive zero knowledge for NP. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *4004 LNCS*(0456717), 339–358. https://doi.org/10.1007/11761679_21

Holt, T. J., & Bossler, A. M. (2020). The palgrave handbook of international cybercrime and cyberdeviance. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, *October*, 1–1489. https://doi.org/10.1007/978-3-319-78440-3

J. Kavitha, G. Indira, A. Anil kumar, A. Shrinita, & D. Bappan. (2024). Fraud Detection in Upi Transactions Using Ml. *EPRA International Journal of Research & Development (IJRD)*, *7838*(April), 142–146. https://doi.org/10.36713/epra16459

LAMGADE, N. (2024). Fraud Detection and Prevention in Financial Institutions. *Interantional Journal of Scientific Research in Engineering and Management*, *08*(04), 1–5. https://doi.org/10.55041/ijsrem32731

Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. *Proceedings - IEEE International Conference on Data Mining, ICDM*, 413–422. https://doi.org/10.1109/ICDM.2008.17

Miller, V. S. (2000). *The use of Elliptic Curves in Cryptography*. *January 1985*, 417–426.

NAGARAJU, M., Babu, P. N., Ravipati, V. S. P., & Chaitanya, V. (2024). *UPI Fraud Detection Using Convolutional Neural Networks (CNN)*. 1–16.

Naik, S. K. L., Kiran, A., Kumar, V. P., Mannam, S., Kalyani, Y., & Silparaj, M. (2024). Fraud Fighters - How AI and ML are Revolutionizing UPI Security. *Proceedings of 2024 International Conference on Science, Technology, Engineering and Management, ICSTEM 2024*, 1–7. https://doi.org/10.1109/ICSTEM61137.2024.10560740

Rani, R., Alam, A., & Javed, A. (2024). Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions. *2024 2nd International Conference on Disruptive Technologies, ICDT 2024*, 924–928. https://doi.org/10.1109/ICDT61202.2024.10489682

ResearchMethodsandProfessionalIssues. (n.d.).

Sundermeyer, M., Schlüter, R., & Ney, H. (2012). LSTM neural networks for language modeling. *13th Annual Conference of the International Speech Communication Association 2012, INTERSPEECH 2012*, *1*, 194–197. https://doi.org/10.21437/interspeech.2012-65

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, *10*(2), 1–19. https://doi.org/10.1145/3298981

https://www.techtarget.com/contributor/Alexander-S-Gillis.

https://us.norton.com/blog/mobile/sim-swap-fraud.

https://brightsec.com/blog/unauthorized-access-risks-examples-and-6-defensive-measures/.

Bodade, R., & Pawade, A. (2023). *Advanced Fraud Detection in Digital Payment Systems*. Journal of Financial Security.

Jagtap, M. (2024). *Applications of Convolutional Neural Networks in Cybersecurity*. International Journal of Advanced AI Research.

Kavitha, R., Sharma, V., & Suresh, K. (2024). *Hidden Markov Models in Fraud Detection: A Comprehensive Analysis*. Journal of Applied Machine Learning.

Lamgade, P. (2024). *AI and Machine Learning Algorithms for Financial Fraud Detection*. Journal of Data Security.

Vasudevan, S., Reddy, M., & Gupta, D. (2024). *Encryption Models and AI in Preventing Digital Fraud*. Journal of Cryptographic Security.