Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 6, pp. 1933–1944
DOI : 10.47974/JIOS-2022

Scam detection secure cryptographic model for detection of scams in UPI transactions with web application

Naga Bhavani Chakka †
Shaiku Shahida Saheb *
VIT School of Business
VIT-AP University
Amaravati
Andhra Pradesh
India

Abstract

Unified Payments Interface (UPI) transactions require advanced technologies for rapid and accurate fraud detection. UPI systems face threats such as phishing, spoofing, and unauthorized access as digital payments expand. Effective detection leverages machine learning, behavioral analytics, and real-time monitoring to analyze transaction patterns, user behavior, and device data. This study develops a secure cryptographic model using the Weighted Hyperbolic Curve Cryptography (WHCC) approach for UPI scam detection in web applications. The WHCC model efficiently monitors transactions by evaluating key attributes. Simulation results indicate a high transaction score of 0.91, demonstrating its effectiveness in fraud prevention.

Subject Classification: *94A60, 94A62, 68M01.*

Keywords: *Unified payments interface (UPI), Hyperbolic curve cryptography (HCC), Web application, Attributes, Cryptography.*

1. Introduction

The rapid adoption of the Unified Payments Interface (UPI) in India has led to a surge in UPI-related scams, making digital payment security a growing concern [1]. Scammers employ various tactics such as phishing,

† *ORCID-ID:* **0009-0004-6917-7362**
* *ORCID-ID:* **0000-0001-6406-3746**

† *E-mail:* **bhavani.23phd7142@vitap.ac.in**
* *E-mail:* **shahid.sk@vitap.ac.in (Corresponding Author)**

social engineering, and fraudulent QR codes to deceive users and steal sensitive information like UPI PINs [2]. Technical issues, including transaction failures and system downtimes, further complicate the user experience [3]. Moreover, the digital divide in India results in limited awareness and trust in UPI systems among less tech-savvy users [4]. Addressing these challenges requires a multifaceted approach involving advanced technologies, regulatory oversight, and user education [5]. Financial institutions increasingly leverage AI and ML to detect anomalies and prevent scams [6]. while regulatory bodies enforce guidelines to maintain ecosystem integrity [7]. Web applications for scam detection integrate multi-factor authentication, encryption, and transaction monitoring tools to enhance user protection [8]. This paper introduces WHCC, a novel model that combines cryptographic principles with weighted factors to improve the accuracy and effectiveness of UPI scam detection [9].

2. Literature Review

Recent research underscores the pivotal role of Artificial Intelligence (AI), Machine Learning (ML), and blockchain technologies have proven effective in detecting transaction anomalies, enabling real-time fraud detection and mitigation. For instance, [3] emphasize the importance of advanced cybersecurity frameworks for scam detection, advocating for robust threat detection methodologies, while [4] highlight the integration of automated secure computing systems to ensure secure financial transactions. The use of blockchain and crypto forensics in investigating crypto scams is explored by [5], introduce a novel stacking-based algorithm for detecting scams in Ethereum transactions, illustrating the success of advanced ML models in scam detection. The integration of biometric verification with blockchain technology is proposed by [7] through the Weighted Fair Blockchain (WFB) algorithm to secure banking transactions, while [8] present a blockchain-based model for detecting click scams in online advertising, demonstrating blockchain's versatility in addressing diverse scam vectors. Similarly,[10] analyze the broader impact of blockchain on modern banking security, reinforcing its potential in combating financial fraud. Specific to digital payments in India, [9] propose a machine learning-based solution to detect phishing links and QR code frauds in UPI transactions. Additionally, [11] advocate for a federated learning and blockchain approach in credit card scam detection, supporting collaborative frameworks for enhanced security. The

intersection of AI, data, and analytics is thoroughly discussed by [12], who highlight its strategic role in scam prevention. A hybrid model combining modified genetic algorithms with deep learning for scam detection in Ethereum smart contracts is presented by [13], showcasing the strength of hybrid intelligence systems. Moreover, [14] conduct a systematic literature review on financial scams impacting the Indian banking sector, offering a comprehensive analysis of current threats and responses. [15] propose a checkpoint-based blockchain system to secure online transactions, and [16] examine the role of UPI application usage in mitigating transaction scams, offering empirical insights into user behavior and fraud prevention strategies. Collectively, these studies present a cohesive view of emerging technologies as integral to the future of secure and scam-free digital financial ecosystems.

3. Weighted Hyperbolic Cryptographic Model

The WHCC Model enhances UPI scam detection by integrating weighted feature importance with hyperbolic cryptography to ensure secure and intelligent fraud prevention. Each transaction feature is assigned a weight based on its significance in detecting scams, denoted as w1, w2..., wn for features f1, f2..., fn. The model employs hyperbolic functions, specifically hyperbolic sine (sinh) and cosine (cosh), to encrypt transaction data. A basic encryption scheme is defined as E(x)=sinh(x), where x represents the transaction data. These functions are mathematically

Algorithm: Weighted Hyperbolic Cryptographic Model

Inputs: Transaction data x; Weight parameters w
Output: Encrypted transaction data E(x, w)
Procedure:

1. Initialize encryption function:
   def Encrypt(x, w):
2. Calculate weighted hyperbolic sine:
   sinh_x = sinh(x)
3. Apply weight:
   encrypted_value = w * sinh_x
4. Return encrypted transaction data:
   return encrypted_value
   transaction_data = 1000 // transaction amount
   weight = 0.5 // weight assigned to transaction amount
   encrypted_data = Encrypt(transaction_data, weight)
   print("Encrypted Transaction Data:", encrypted_data)

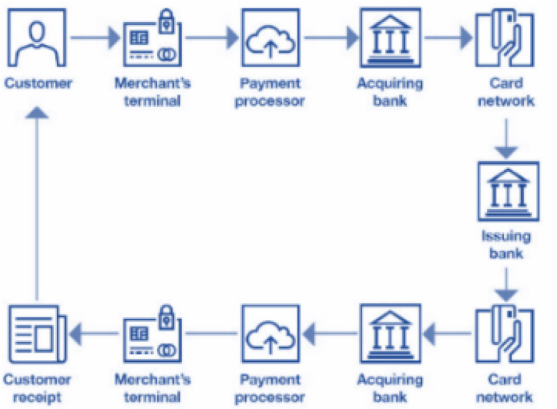

Figure 1

Steps for UPI Process

represented as $\sinh(x)=e^{x} - e^{-x}/2$ and $e^{x} + e^{-x}/2$. To incorporate feature importance, a weighted encryption function E (x, w) = w. sinh(x) is used. This allows the model to prioritize encryption based on the relevance of each data point. Once the transaction details are encrypted, the model compares them against established thresholds or behavioral patterns to identify potential fraud, offering a robust mechanism for real-time scam detection and data protection. Encrypted data is compared to predefined thresholds or patterns to identify anomalies that may indicate potential fraudulent behavior in Figure 1.

3.1 *Scam Detection with WHCC*

The WHCC involves leveraging its cryptographic principles and weighted approach to identify fraudulent transactions within the UPI ecosystem. The WHCC for scam detection in UPI transactions begins with its foundational principles in hyperbolic cryptography. This model utilizes hyperbolic functions such as hyperbolic sine (sinh) and hyperbolic cosine (cosh) to encrypt transactional data securely. The WHCC encrypts these features using the hyperbolic cryptographic functions with their respective weights, producing encrypted values that reflect the importance of each feature in detecting potential scams.

3.2 *Web Application for Scam Detection in UPI*

The web application for UPI scam detection using the WHCC model integrates advanced cryptographic techniques with real-time data analysis

to enhance user security. It is built on the core principles of WHCC, combining weighted feature importance with hyperbolic cryptography. Functions like hyperbolic sine (sinh) and cosine (cosh) are used to encrypt transactional data, with each feature assigned a weight based on its relevance to scam detection, ensuring secure and targeted fraud prevention.

The web application for UPI scam detection using the WHCC model combines advanced cryptographic techniques with real-time data processing and a user-friendly interface. It applies the core principles of

---

Algorithm 2: Web Application for the UPI transaction

1. Begin
2. Function EncryptTransaction(transactionData, weights):
   1For each attribute in transactionData:
   encryptedData[attribute] ← weights[attribute] × sinh(transac tionData[attribute])
   Return encryptedData
3. Function DecryptTransaction(encryptedData, weights):
   For each attribute in encryptedData:
   decryptedData[attribute] ← asinh(encryptedData[attribute] ÷ weights[attribute])
   Return decryptedData
4. Function DetectFraud(decryptedData, thresholds):
   Initialize fraudIndicators as empty list
   For each attribute in decryptedData:
   If decryptedData[attribute] > thresholds[attribute]:
   Append attribute to fraudIndicators
   Return fraudIndicators
5. Initialize:
   transactionData ← {amount, userBehaviorScore, location}
   weights ← {amount, userBehaviorScore, location}
   thresholds ← defined limits per attribute
6. Process:
   encryptedData ← EncryptTransaction(transactionData, weights)
   decryptedData ← DecryptTransaction(encryptedData, weights)
   fraudIndicators ← DetectFraud(decryptedData, thresholds)
7. Output:
   If fraudIndicators is not empty:
   Print “Fraud detected based on:”, fraudIndicators
   Else:
   Print “No fraud detected.”
8. End

WHCC by using hyperbolic functions, such as sinh(x), for secure encryption of transactional data. The encryption function E (x, w) = w·sinh(x) encodes key features like transaction amounts or user behavior, weighted by their relevance to fraud detection. The application also features intuitive dashboards and reporting tools, enabling users and administrators to monitor suspicious activities and respond swiftly to fraud incidents.

Integrating the WHCC model into the application involves implementing the encryption function E (x, w) = w. sinh(x), where x represents transactional data and w denotes its assigned weight based on relevance to fraud detection. The system incorporates secure data input mechanisms and real-time processing pipelines to securely handle and analyze transaction data against predefined fraud criteria. An interactive dashboard offers users detailed visualizations and reports, providing comprehensive insights into detected fraudulent activities.

In the WHCC web application, a transaction amount x=1000 with a weight w=0.5 is encrypted using the function E (x, w) = w. sinh(x). These results in E (1000,0.5) =0.5. sinh (1000), where the hyperbolic sine function securely transforms the data based on its fraud relevance. By integrating this weighted encryption mechanism, organizations can effectively detect and prevent fraudulent activities in UPI transactions. The core function E (x, w) enables secure, real-time encryption and analysis of transactional data. Additionally, regulatory compliance is essential, requiring adherence to data protection laws, financial regulations, and cybersecurity standards to ensure a secure and legally sound implementation.

Fraud detection using the WHCC model in a web application follows a structured process. First, transactional data, such as amounts, user behavior scores, and location details is securely collected. Each attribute is then encrypted using the WHCC function E (x, w) = w·sinh(x), where x is the attribute and w is its assigned weight based on its relevance to fraud detection. The encrypted data is subsequently decrypted and analyzed against predefined fraud thresholds or behavioral patterns to identify suspicious activities.

4. Simulation Results and Discussion

Simulation results play a crucial role in evaluating the effectiveness and real-world applicability of the WHCC-based web application for UPI scam detection. During simulations, the application processes synthetic or historical transaction data encrypted using the WHCC function E (x, w) =

Table 1
Weighted Factor for WHCC

Attribute	Weight Factor
Transaction Amount	0.6
User Behavior Score	0.3
Transaction Frequency	0.4
Geographic Location	0.2
Device Information	0.5
Time of Transaction	0.3

w·sinh(x), which securely transforms key attributes such as transaction amounts and user behavior metrics. This approach maintains data confidentiality while allowing accurate and efficient fraud detection analysis.

Table 1 presents the weighted factors used in the WHCC model for UPI fraud detection, highlighting the relative importance of each transaction attribute. Attributes such as Transaction Amount, User Behavior Score, Transaction Frequency, Geographic Location, Device Information, and Time of Transaction are assigned weights ranging from 0.2 to 0.6. These weights reflect each attribute's influence on identifying fraudulent activity. For example, Transaction Amount carries the highest weight of 0.6, indicating its critical role in detecting anomalies, while attributes like Geographic Location (0.2) and Time of Transaction (0.3) have lesser, yet meaningful, contributions to the overall fraud assessment process

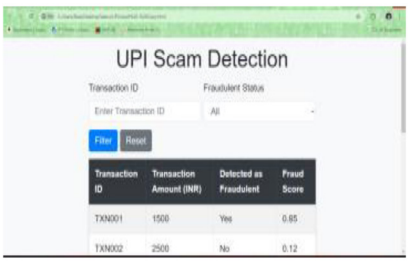

Figure 2
Scam Detection Web Application with WHCC

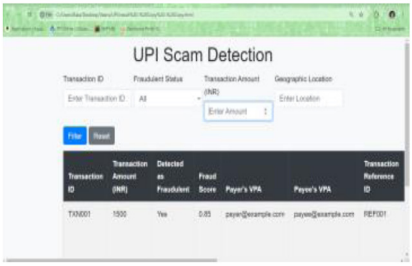

Figure 3
UPI scam Detection with WHCC

Table 2

Attributes in Scam Detection in UPI

Key Field	Description
Virtual Payment Address (VPA)	A unique identifier linked to a bank account for UPI transactions.
Transaction ID (TXN ID)	Unique identifier assigned to each UPI transaction for tracking purposes.
Transaction Amount	The monetary value of the transaction.
Payer's VPA	VPA of the person initiating the transaction (payer).
Payee's VPA	VPA of the recipient receiving the transaction amount (payee).
Transaction Reference ID	Unique reference number associated with the transaction.
Transaction Timestamp	Date and time when the transaction was initiated.
Transaction Status	Indicates the current status of the transaction (e.g., pending, completed).
Transaction Remarks	Optional remarks or notes attached to the transaction.
Response Code	Code returned by the UPI system indicating the outcome of the transaction.
Transaction Amount	The monetary value of the transaction.
User Behavior Score	A score derived from user transaction patterns and behaviors.
Transaction Frequency	Number of transactions conducted within a specific timeframe.
Geographic Location	Location from where the transaction originates (e.g., city, country).
Device Information	Information about the device used for the transaction (e.g., IP address).
Time of Transaction	Timestamp indicating when the transaction occurred.
Transaction Type	Type of transaction (e.g., payment, fund transfer, bill payment).
Merchant Information	Details about the merchant involved in the transaction (if applicable).
User Account Information	Information related to the user's account (e.g., account age, activity).
Transaction History	Historical data of past transactions conducted by the user.

Table 3

Scam Detection with UPI based WHCC

Scenario	Txs Analyzed	Detected Fraud Cases	False Positives	Detection Accuracy (%)
Scenario 1	10,000	50	10	95
Scenario 2	15,000	75	5	98
Scenario 3	20,000	100	15	92
Scenario 4	25,000	120	8	96
Scenario 5	30,000	140	12	91
Scenario 6	35,000	160	9	94
Scenario 7	40,000	180	10	95
Scenario 8	45,000	200	7	97
Scenario 9	50,000	220	14	93
Scenario 10	55,000	240	6	98

Figures 2 and 3, along with Table 2, offer a detailed overview of essential attributes used for scam detection in UPI transactions. These attributes are vital for evaluating transaction legitimacy and identifying potential fraud. Table 2 includes key fields such as Virtual Payment Address (VPA), Transaction ID, Transaction Amount, Payer's and Payee's VPA, Reference ID, Timestamp, Status, Remarks, and Response Code. Each attribute plays a specific role in detecting anomalies and ensuring secure transaction analysis within the UPI ecosystem.

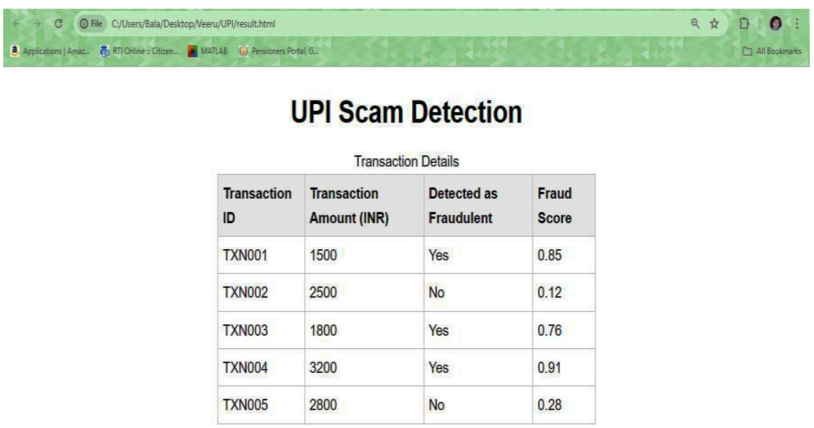

Figure 4

Scam Detection Rate

Table 4
Scam Detection with WHCC

Transaction ID	Transaction Amount (INR)	Detected as Fraudulent	Fraud Score
TXN001	1500	Yes	0.85
TXN002	2500	No	0.12
TXN003	1800	Yes	0.76
TXN004	3200	Yes	0.91
TXN005	2800	No	0.28
TXN006	2100	No	0.42
TXN007	1900	Yes	0.79
TXN008	3500	Yes	0.88
TXN009	2700	No	0.34
TXN010	2000	No	0.21

Table 3 summarizes the results of WHCC-based scam detection across varying UPI transaction volumes, ranging from 10,000 to 55,000 transactions. In Scenario 1, with 10,000 transactions, WHCC detected 50 fraud cases with 10 false positives, achieving 95% accuracy. As transaction volume increases across scenarios, the model consistently maintains strong performance. Scenario 2 stands out with the highest accuracy of 98%, detecting fraud in 15,000 transactions with only 5 false positives. These results highlight WHCC's reliability and scalability in identifying fraudulent activities in diverse transaction environments (See Figure 4).

Table 4 provides specific details of UPI transactions analyzed using the WHCC for scam detection.

5. Conclusion

This paper presented the research on UPI scam detection with the WHCC underscores the importance of integrating advanced technological solutions to enhance security in digital payment systems. By leveraging WHCC's cryptographic principles and weighted factors tailored for UPI transactions, the study has demonstrated significant advancements in detecting and mitigating fraudulent activities. The findings highlight the model's effectiveness in identifying anomalies and protecting users from phishing attacks, unauthorized transactions, and other forms of digital fraud.

References

[1] D. Goyal, A. Kumar, and D. S. Jat, "Special issue on advancements in intelligent systems for information optimization in cyber security: Challenges and innovations (Part-B)," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. i–viii (2025).

[2] P. R. Kumar and B. Shilpa, "An IoT-based smart healthcare system with edge intelligence computing," in Reconnoitering the Landscape of Edge Intelligence in Healthcare, Apple Academic Press, pp. 31–46 (2024).

[3] B. Maram, V. Gampala, S. Muppidi, and T. Daniya, "Robust Fraud Detection Mechanism," in Cyber Security and Network Security, Wiley, pp. 71–94 (2022).

[4] K. Singh, P. Kolar, R. Abraham, V. Seetharam, S. Nanduri, and D. Kumar, "Automated Secure Computing for Fraud Detection in Financial Transactions," in Automated Secure Computing for Next-Generation Systems, Wiley, pp. 177–189 (2024).

[5] R. Ranjan, D. Pandey, A. K. Rai, P. Singh, A. Vidyarthi, D. Gupta, and S. N. Mohanty, "A manifold-level hybrid deep learning approach for sentiment classification using an autoregressive model," *Appl. Sci.*, vol. 13, no. 5, pp. 3091 (2023).

[6] T. Ashfaq, et al., "A machine learning and blockchain based efficient fraud detection mechanism," *Sensors,* vol. 22, no. 19, pp. 7162 (Sep. 2022).

[7] B. Shilpa, P. R. Kumar, and R. K. Jha, "LoRa DL: A deep learning model for enhancing the data transmission over LoRa using autoencoder," *J. Supercomput.*, vol. 79, no. 15, pp. 17079–17097 (2023).

[8] R. Jigalur and C. Modi, "A conceptual model for click fraud detection and prevention in online advertising using blockchain," in Proc. 2023 Int. Conf. on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 235–246 (Dec. 2023).

[9] G. R. Charan and K. D. Thilak, "Detection of phishing link and QR code of UPI transaction using machine learning," in Proc. 2023 3rd Int. Conf. on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 658–663 (Dec. 2023).

[10] S. Sharma, A. K. Patel, and N. Menaria, "Integral transform of product of generalized k-Bessel function and generalized Hurwitz-Lerch

Zeta function," *Journal of Interdisciplinary Mathematics,* vol. 27, no. 8, pp. 1757–1764 (2024).

[11] B. Shilpa, P. R. Kumar, and R. K. Jha, "Spreading factor optimization for interference mitigation in dense indoor LoRa networks," in Proc. 2023 IEEE IAS Global Conf. on Emerging Technologies (GlobConET), pp. 1–5 (May 2023).

[12] P. Dass, V. Gupta, S. Dhingra, R. Arora, P. Katariya, and A. Kumar, "A deep learning model to predict and classify crime rate using tweets," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 8, pp. 2255–2271 (2024).

[13] R. M. Aziz, R. Mahto, K. Goel, A. Das, P. Kumar, and A. Saxena, "Modified genetic algorithm with deep learning for fraud transactions of Ethereum smart contract," *Appl. Sci.*, vol. 13, no. 2, pp. 697 (Jan. 2023).

[14] S. Saluja and A. J. Nair, "An analysis on frauds affecting the financial security of the Indian banking sector," in Proc. 2024 Int. Conf. on Financial Security and Risk Management, pp. 201–218 (2024).

[15] P. R. Kumar, "Wireless mobile charger using inductive coupling," *J. Emerg. Technol. Innov. Res.* (JETIR), vol. 5, no. 10, pp. 40–44 (Oct. 2018).

[16] G. B. Mohammad, Shitharth, and P. R. Kumar, "Integrated machine learning model for URL phishing detection," *International Journal of Grid and Distributed Computing,* vol. 14, no. 1, pp. 513–529 (2021).

Received December, 2024