

DeepTrust-UPI: A Quantum Resistant AI Architecture for Deepfake Based Fraud Detection in UPI Transactions

Ankitha R¹, Pruthvi Ramachandra Hegde²

^{1,2}Student, Department of Computer Science and Business Systems, K.S. School of Engineering and Management, Bengaluru, Karnataka, India

Abstract

With the advent of digital payment methods, there have been many changes in the field of financial transactions with the Unified Payments Interface (UPI) of India being one of the most adopted real-time payments in the world. In parallel to this, there has been an increased usage of AI by cybercriminals to carry out fraud attacks that include deepfake identity impersonation, synthetic voice manipulation, facial recognition, and social engineering frauds. Such attacks reveal the drawbacks of the existing fraud detection system which is more concerned about transaction anomalies rather than multimodal attacks. Moreover, the advancement of quantum computing adds another layer of security threat to the existing cryptographic systems.

The present paper introduces DeepTrust-UPI – a novel post-quantum secure AI framework to detect deepfake-assisted fraud in UPI transactions with the help of an integrated multimodal security architecture. The suggested framework leverages three intelligent detection modules, which include machine learning-based transaction anomaly detection, deepfake audio detection based on spectrogram and deep neural networks, and deepfake video detection leveraging convolutional neural networks. These outputs are then fused by a centralized risk analysis engine to compute a fraud score for each transaction. Post-quantum cryptographic mechanisms ensuring long-term confidentiality and secure communication are implemented to protect sensitive information from potential attacks using quantum computers.

In contrast to the current approach, which considers either transaction fraud detection or multimedia forgery separately, DeepTrust-UPI combines behavioral analytics, biometric verification, and post-quantum cryptography in a single architectural solution. While at this moment the presented research is conceptual in nature and based on simulated implementation scenarios, this work shows the possibility of developing such a system that combines advanced fraud detection based on AI with next-generation security protection. It is expected that the framework will improve fraud detection accuracy, reduce false positives, increase user confidence, and provide the decision-support layer for future digital payments.

Keywords: Unified Payments Interface (UPI), Deepfake Detection, Financial Fraud Detection, Artificial

Intelligence, Machine Learning, Post-Quantum Cryptography, Cybersecurity, Digital Payments, Multimodal Authentication.

1. Introduction

During the past decade, digital transformation had a huge impact on the financial industry by allowing individuals and organizations to conduct secure and instant money transactions with the help of digital payments. Among the innovative financial instruments, the Unified Payments Interface (UPI) developed by National Payments Corporation of India (NPCI) became one of the most successful in the world. UPI provides a convenient, interoperable, and always-available payment infrastructure, thus contributing to India's transition towards becoming a cashless economy.

Nevertheless, the great success of modern digital payment systems was accompanied by growing number of increasingly sophisticated cyber attacks. Cyber criminals started to leverage artificial intelligence tools to create new attack vectors able to bypass existing security measures. In particular, one of the most rapidly developing areas of modern attack vectors includes the usage of deepfake technology, which allows generating synthetic audio and video that mimics authentic users using generative adversarial network architectures [9]. Nowadays, deepfake generation technologies, including those created on the base of large generative models, are capable of replicating facial expressions, voices, lip syncs and other elements with a high degree of accuracy [9, 11].

The most recent examples of cyber-crime include the use of cloned voices for pretending to be a relative, a bank employee or a company CEO and the ability of the AI generated videos to trick video-based KYC system. In fact, both cases are very dangerous because of the exploitation of human factors, not the software bugs. However, the current fraud detection tools are focused on transaction history, spending habits, geographical area and some predefined behavioral rules. Although the current approach is very efficient in terms of recognizing suspicious financial transactions, it is still unable to detect the sophisticated multimedia attacks.

In addition, there is a problem of cryptographic security in the future. Modern digital payment systems use classical public-key cryptography algorithms such as RSA and Elliptic Curve Cryptography (ECC). Both of the mentioned methods are still resistant to any computational attack by the classical computers. At the same time, the fast progress in the field of quantum computing will make these algorithms vulnerable in the future. Quantum algorithms, like Shor's algorithm, have a potential to break down widely used public-key cryptographic methods. For this reason, payment systems must be prepared for the migration to the Post-Quantum Cryptography (PQC) which uses quantum-resistant algorithms for keeping confidentiality in the era of large quantum computers.

Thus, the discussed issues need to be addressed in the context of unified intelligent security solution which will take into account financial behavior, multimedia security and secure communications.

For this reason, this paper proposes a novel AI-based approach called DeepTrust-UPI. The approach provides an integrated solution for the transaction anomaly detection, deepfake audio verification, deepfake video verification and post-quantum cryptographic protection in the form of one modular framework. Thus, DeepTrust-UPI constantly checks transaction behavior, verifies multimedia using deep

learning techniques and ensures secure communication using quantum-resistant cryptographic methods. This combination allows improving the efficiency of the fraud detection, lowering the number of false alarms and creating a future-oriented security architecture of digital payment systems.

The major contributions of this research are as follows:

- Implementation of multimodal AI technology based on analysis of transactions, speech, and face identification.
- Inclusion of post-quantum cryptography technologies to increase the security of payments in the long term.
- Creating a modular architecture that will allow implementing banking API and other solutions in the future.
- Introduction of a risk fusion engine that will use several types of evidence for detection of fraud.
- Creation of the conceptual base for implementation of next generation AI-enabled digital payment ecosystem.

2. Literature Review

The swift pace of development of AI technology has influenced not only cybersecurity but also the practices of cybercriminals [12]. Numerous methods of deepfake detection, fraud detection in financial transactions, and cryptography improvement have been proposed by the researchers during recent years. However, despite the success that has been achieved in each of the fields separately, there is a lack of research on creating an integrated system for digital payment security.

Deepfake detection is becoming one of the most active fields of study in computer vision and multimedia forensics. The recent studies use the Convolutional Neural Networks (CNNs), Vision Transformers (ViTs) [10], temporal features extraction, frequency domain analysis, and explainable AI [5] in order to separate the real media from the synthetic ones which are mostly produced with the help of the techniques of generative adversarial networks [9]. CNN-based techniques are based on detection of inconsistent faces, illumination effects, abnormalities in eye blinking, and compression signatures in images while the transformer architecture takes into consideration long-range dependencies in videos [10]. Deep learning spectrogram models also showed excellent results in recognizing AI-generated voices by examining frequency distribution and acoustic temporal features. However, many of the techniques are quite computationally expensive and demonstrate poor generalization ability to deal with unknown deepfake generation techniques.

Detection of financial frauds has progressed from the simple rule-based models to the intelligent machine learning models which are able to adaptively detect anomalies. Such algorithms as Random Forest, XGBoost, Support Vector Machines, Isolation Forest, and Graph Neural Networks (GNNs) have been successfully used to detect financial transactions with suspicious activity [1, 2, 3, 4]. They operate with such factors as customer spending habits, transaction frequency, transfer amount, temporal patterns, and network structure in order to identify the frauds [1, 3]. Despite the effectiveness in transaction monitoring, the current systems work solely with the structured financial data and seldom use biometric verification or multimedia authentication, therefore making them vulnerable to impersonation attacks due to the AI-

generated media [4].

Simultaneously with that, some achievements have been made in post-quantum cryptography. Such cryptography approaches as lattice-based, hash-based, multivariate polynomial, and code-based algorithms resistant to quantum attacks were proposed by the researchers [6]. The process of standardization sped up the creation of efficient algorithms resistant to quantum attacks that can be used in future [6, 7]. Hash-based methods such as SHA-3 were improved to support secure multimodal biometric authentication [8]. Nevertheless, existing researches concentrate mainly on secure communication and key exchange and do not combine cryptographic resistance in the intelligent fraud detection systems [6, 7].

Summarizing the results of the current researches, one can state that a significant research gap exists. Most of the systems concentrate on just one of the aspects of payment security: transaction anomaly detection, deepfake detection, or cryptography. Very few works examine the use of all three techniques together in an integrated system. That is why there is a motivation to create the proposed DeepTrust-UPI framework that will incorporate all of the technologies into one secure and scalable system.

Table 1: Summary of Related Work

Title	Authors	Publication	Summary	Methodology	Results	
Multi-Layer UPI Fraud Detection Using Machine Learning	Amrutha Podipireddy et al.	IEEE, 2025	Proposed a hybrid fraud detection framework for UPI systems using supervised and unsupervised ML techniques.	Combined Random Forest, XGBoost, Isolation Forest, and clustering methods for fraud detection.	Improved detection of both known and unknown frauds with real-time alerts.	Dete
Enhancing Digital Payment Security using	Dr. N. Lingareddy et al.	IEEE, 2025	Developed an adaptive fraud detection system for secure UPI transactions.	Integrated DQN-based reinforcement learning with XGBoost classification.	Achieved 98.7% accuracy with low false positive rate and latency.	accu lea

Title	Authors	Publication	Summary	Methodology	Results	
Advanced ML Algorithms						
Secure UPI: ML-Driven Fraud Detection System	Rupa Rani et al.	IEEE, 2024	Focused on real-time fraud detection in digital payment systems using machine learning.	Used XGBoost feature analysis for fraud classification.	Improved transaction monitoring and fraud prediction accuracy.	Sur
Data Anomaly Detection Based on Isolation Forest Algorithm	Liang Zhang et al.	IEEE, 2022	Proposed anomaly detection using Isolation Forest for identifying abnormal behavior.	Applied PCA with Isolation Forest for anomaly detection and preprocessing.	Efficiently identified anomalous transaction patterns.	unsu r
Multi-Model Financial Fraud Detection with Explainable AI	Anusha Khot et al.	IJFMR, 2025	Introduced explainable AI for interpretable fraud detection.	Combined ML models with Explainable AI techniques.	Improved interpretability and transparency in fraud analysis.	En expl pre
Post-Quantum Cryptography: Review of Techniques	Ritik Bavdekar et al.	IEEE, 2023	Reviewed quantum-resistant cryptographic techniques for security.	Analyzed lattice-based, code-based, and hash-based PQC algorithms.	Identified secure approaches resistant to quantum attacks.	Pro s q to
Post-Quantum Cryptography for Critical Infrastructure	Pankaj Chandre et al.	IEEE, 2024	Proposed secure PQC frameworks for protecting critical digital infrastructure.	Developed hybrid post-quantum cryptographic architecture.	Enhanced resistance against future quantum-based cyber threats.	inf
SHA-3 for FPGA-Based Multimodal Biometric Authentication	M. M. Sravani et al.	IEEE Transactions, 2022	Enhanced SHA-3 architecture for secure biometric authentication systems.	Optimized FPGA-based SHA-3 implementation for multimodal authentication.	Achieved high throughput and improved authentication efficiency.	andau

3. Research Gap

Although considerable progress has been made in the development of artificial intelligence, cybersecurity, and fraud detection systems, most existing research works only attempt to solve particular security issues rather than offering an integrated solution that could be applied to modern digital payment systems. Deepfake detection models demonstrate excellent results when detecting and classifying manipulated audio and video content using deep learning techniques such as CNNs, ViTs, and frequency domain processing. At the same time, machine learning techniques have shown great performance in fraud detection using transaction history and behavior analysis. In addition, research works in Post-Quantum Cryptography field propose encryption algorithms that could be used to protect future communication infrastructure from potential quantum attacks.

Nevertheless, all these technologies remain independent in development, thus, creating a fragmented security environment. Most existing fraud detection systems work with structured data only, ignoring multimedia authentication at all. Similarly, most deepfake detection systems do not consider financial transactions at all, which makes them useless for payments ecosystem. Finally, post-quantum cryptography is usually limited only to creating secure communication channels without additional features of intelligent fraud detection or user authentication.

Thus, there is a research gap related to the lack of an integrated technology solution that could perform several different tasks including transaction behavior analysis, multimedia authentication, and post-quantum cryptography. Since hackers often use artificial intelligence to create deepfakes and commit financial fraud, such an isolation of technologies becomes inadequate.

DeepTrust-UPI framework proposed in this research aims to fill this research gap by introducing integrated transaction anomaly detection, deepfake audio detection, deepfake video verification, and post-quantum cryptography into one multimodal system.

4. Problem Statement

The quick deployment of the Unified Payments Interface (UPI) has revolutionized digital finance through provision of fast and secure payment solutions. However, this wide deployment has made these digital payment platforms vulnerable to more sophisticated cyber-attacks. The conventional techniques of detecting fraud include analysis of the transaction history, set behavioral rules, and statistical detection of anomalies. While these techniques are useful for detecting normal forms of fraud, they are ineffective in detecting AI-generated attacks using synthetic media such as deepfake videos and voice cloning.

The current cyber criminals are taking advantage of deepfake technology to pretend to be legitimate users in the process of authentication, fool customer support staffs, trick the biometric verifiers, and perform social engineering attacks. This type of cyberattacks is hard to detect since the multimedia generated is very similar to real users' identities.

Apart from multimedia impersonation, another major issue is the insecurity of classical public key cryptographic algorithms. With the advancement in large-scale quantum computing, there is the danger of breaking currently widely accepted encryption schemes such as RSA and ECC. Hence, the digital payment platforms require security mechanisms that can protect them from the existing AI-enabled fraud attacks and the future cryptographic attacks enabled by quantum computers.

This means that there is an urgent need to create a framework that combines the two aspects of multimodal fraud detection and quantum cryptography security to establish trustworthiness, scalability, and future-readiness of digital payment platform.

5. Objectives

The main goal of this research is to come up with an intelligent and secure AI-based framework that can detect fraud using deepfakes in UPI payment transactions and offer cryptographic protection against quantum computer attacks.

Specific Objectives

- Build a machine learning algorithm to detect any abnormal transaction patterns.
- Detection of AI-generated fake audio using deep learning models based on spectrograms.
- Detection of tampered video faces using Convolutional Neural Networks.
- Combine transaction detection, audio validation, and video face detection in one risk management framework.
- Protecting sensitive communications through Post-Quantum Cryptographic algorithms.
- Lower the incidence of false positives using multimodal data fusion.
- Create an alert mechanism for fraudulent transactions in real time.
- Create a modular system design to facilitate future additions.

6. Existing System vs Proposed System

Table 2: Comparative Study of the Existing and Proposed System

Parameter	Existing Fraud Detection Systems	Proposed DeepTrust-UPI Framework
Fraud Detection	Transaction anomalies only	Transaction + Audio + Video
Authentication	OTP, PIN, Device ID	AI-based Multimodal Authentication
Parameter	Existing Fraud Detection Systems	Proposed DeepTrust-UPI Framework
Deepfake Detection	Not Supported	Integrated Audio & Video Detection
Machine Learning	Single ML Model	Multiple AI Models with Risk Fusion
Security Mechanism	Classical Cryptography	Post-Quantum Cryptography
Decision Making	Rule-Based	AI-Assisted Risk Analysis
Scalability	Limited	Modular Architecture
False Positives	Comparatively Higher	Reduced through Evidence Fusion
Future Readiness	Vulnerable to Quantum Computing	Quantum-Resistant Design

It is evident from the above comparative study that the existing fraud detection systems for UPI are predominantly transactional based and use security rules. Although such systems function effectively in case of traditional forms of financial frauds, they do not have the capability to detect multimedia-based impersonations or any future cryptographic attacks. The DeepTrust-UPI model solves these problems by utilizing intelligent multimodal techniques along with quantum security measures.

7. Proposed Framework

The proposed DeepTrust-UPI framework consists of a hierarchical architecture that integrates artificial intelligence, machine learning, deep learning, and post-quantum cryptography for the development of an advanced fraud detection mechanism. This solution will not replace the current banking architecture but will work on top of it in order to verify the authenticity of transactions.

The architecture contains six principal components, which are:

7.1 User Interaction Layer

This layer takes in transaction requests made via the mobile UPI apps. Apart from the transaction information, this framework may also take in biometric information for any risky transactions. Such information includes voice and facial verification.

7.2 Transaction Analysis Module

Transaction analysis consists of analyzing behavioral traits such as:

- Transaction amount
- Transaction frequency
- Device fingerprint
- Login location
- Time of transaction
- Merchant category
- Historical user behavior

Machine learning is used to detect such attributes in order to check for anomalies in the transactions of users.

7.3 Audio Deepfake Detection Module

In the case where voice authentication is needed, the user's voice is transformed into spectrograms and processed using deep learning models, where features such as the following are extracted:

- Frequency spectrum
- Pitch variation
- Temporal consistency
- Harmonic distortion
- Synthetic speech artifacts

The features above help the system to differentiate between real voices and AI-created voice imitations.

7.4 Video Deepfake Detection Module

When performing facial verification, the system captures video frames which are then preprocessed and

analyzed by the Convolutional Neural Network, which detects the following visual anomalies:

- Facial landmark abnormalities
- Eye blinking irregularities
- Lip synchronization errors
- Illumination inconsistencies
- Compression artifacts
- Frame-level manipulation patterns

This generated confidence measure indicates the probability of face tampering.

7.5 Risk Fusion Engine

The results obtained from the modules of transaction analysis, audio authentication, and video authentication are submitted to the central Risk Fusion Engine. Rather than depending on one detection outcome, the fusion engine takes into account the findings from all three of them to estimate the likelihood of fraud. The transaction is then placed in one of three categories:

- Safe Transaction
- Suspicious Transaction
- Fraudulent Transaction

The above multimodal decision-making process will improve reliability greatly while reducing false alarms.

7.6 Post-Quantum Security Module

In order to safeguard sensitive communication among system modules, the DeepTrust-UPI has Post-Quantum Cryptography algorithms in place for encryption and authentication. This module offers:

- Quantum-resistant encryption
- Secure authentication
- Protected key exchange
- Long-term confidentiality
- Future-ready communication security

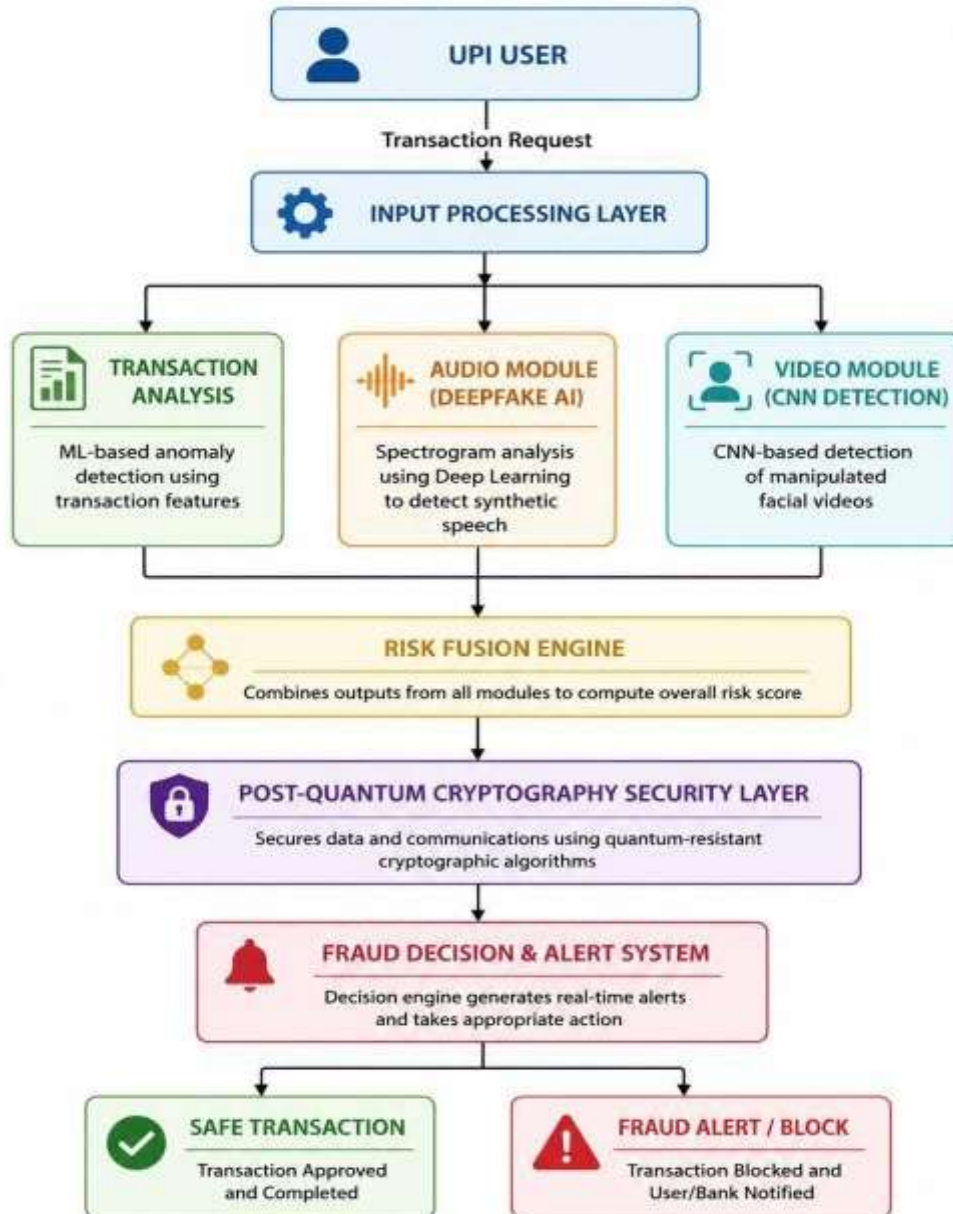
Through the use of intelligence-based fraud detection and quantum encryption, the new system is resilient to existing and future quantum attacks.

The architecture for DeepTrust-UPI shows how transaction requests proceed through three different detection modules which include: transaction analysis, audio deepfake detection, and video deepfake detection. These outputs are fused by the central Risk Fusion Engine. Afterward, a decision is made and the result encrypted via the Post-Quantum Cryptography layer before the system proceeds to either approve the transaction or issue a fraud alert.

8. Proposed System Architecture

Figure 1 depicts the layered architecture of the proposed DeepTrust-UPI system showing the transaction requests passing through the three detection modules, Risk Fusion Engine, Post-Quantum Cryptography Security Layer, and finally Fraud Decision and Alert System.

Figure 1: Proposed DeepTrust-UPI System Architecture



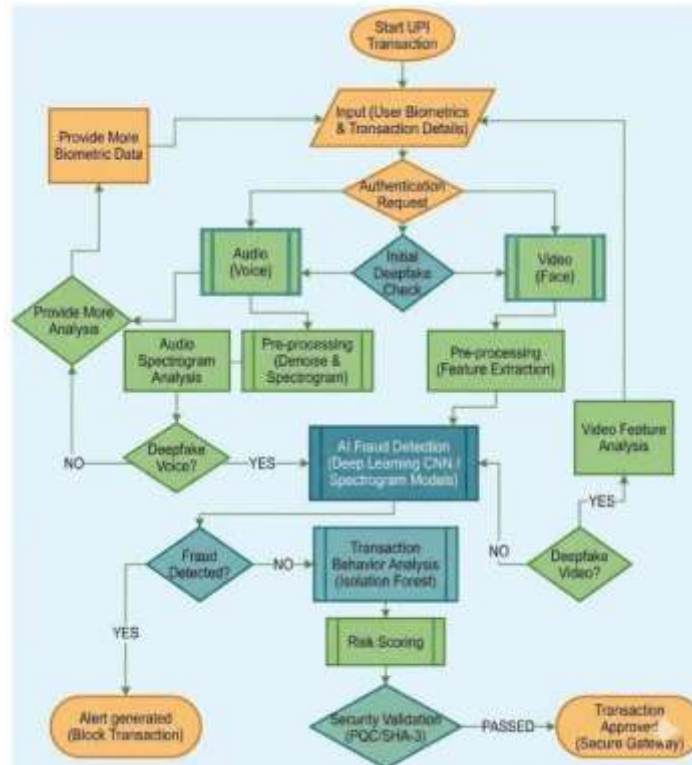
9. Methodology

The proposed DeepTrust-UPI system employs a multi-modal security approach which is aimed at improving the fraud detection process for Unified Payments Interface (UPI) transactions by utilizing transaction anomaly analysis, audio deepfake detection, video deepfake verification, and post-quantum cryptography. The proposed DeepTrust-UPI system is conceived as a decision support system that will combine multiple evidences to verify the authenticity of a transaction.

The methodology involves seven different phases starting from data acquisition to transaction decision-

making.

Figure 2: Proposed DeepTrust-UPI Framework Methodology Flowchart



9.1 Phase 1: Data Acquisition

In the proposed approach, three types of input data are considered.

1. Transaction Data

Transaction-related information may include:

- Transaction Amount
- Transaction Time
- UPI ID
- Merchant Details
- Device Information
- Geographic Location
- Transaction Frequency
- Historical User Behaviour
- Failed Authentication Attempts

These characteristics are used to collect behavioural data needed for anomaly detection.

2. Audio Authentication

For transaction flagged as risky, the proposed approach includes an optional voice authentication procedure where the recorded audio signal is preprocessed and then analyzed for fake speech detection.

3. Video Authentication

In risky operations, the architecture might demand facial verification by extracting video frames and

analysing them for visual manipulation linked to deepfake attacks.

9.2 Phase 2: Preprocessing of Data

Preprocessing is performed on each data type prior to feature extraction to improve the data quality.

Transaction Data

Preprocessing steps suggested here include:

- Missing value handling
- Outlier detection
- Feature normalization
- Feature scaling
- Label encoding
- Data balancing

Audio Data

The voice samples can be represented as Mel spectrograms or any other acoustic representation like MFCC features.

Video Data

Video frames may undergo:

- Face Detection
- Face Alignment
- Image Resizing
- Frame Normalization
- Facial Landmark Detection

Facial regions that have been recognized only are sent for further processing.

9.3 Stage 3: Feature Extraction

The proposed method extracts discriminatory features from each individual modality of input.

Transaction Features

Behavioural features may include:

- Average Transaction Amount
- Daily Spending Pattern
- Transaction Velocity
- Merchant Similarity
- Device Consistency
- Geographic Consistency
- Time-based Behaviour

Audio Features

Possible acoustic features include:

- MFCC Coefficients
- Pitch
- Spectral Centroid
- Chroma Features

- Zero-Crossing Rate
- Harmonic Energy

These features have been utilized extensively for speech synthesis.

Video Features

Visual features may include:

- Facial Embeddings
- Eye Blink Frequency
- Lip Synchronization
- Head Movement
- Texture Inconsistencies
- Compression Artifacts
- Frequency-domain Features

10. Proposed AI Models

The DeepTrust-UPI methodology suggests the use of distinct Artificial Intelligence models for fraud detection tasks.

10.1 Transaction Anomaly Detection

Some supervised and unsupervised machine learning techniques can be employed, which include:

- Random Forest
- XGBoost
- Isolation Forest
- Logistic Regression
- Support Vector Machine

Of these, the XGBoost technique appears to be a good choice owing to its efficient handling of structured financial data and class imbalance issues. Ultimately, the algorithm needs to be selected during future experimentation.

10.2 Audio Deepfake Detection

The framework includes the processing of Mel spectrogram representation through CNN or related deep learning algorithms that will help differentiate the actual speech from artificial voices.

10.3 Video Deepfake Detection

Facial verification can be done by deepfake detection models based on CNN that will identify the abnormalities in the face like unusual texture, lip sync issues, compression artefacts, and other temporal irregularities that can be found in manipulated videos.

11. Multimodal Risk Fusion

Rather than using one detection technique, the proposed framework uses the output of transaction analysis, audio verification, and video verification to produce the overall fraud risk score. Here, let us use T for Transaction Risk Score, A for Audio Deepfake Score, and V for Video Deepfake Score.

$$R = w^1T + w^2A + w^3V \quad (1)$$

$$w^1 + w^2 + w^3 = 1 \quad (2)$$

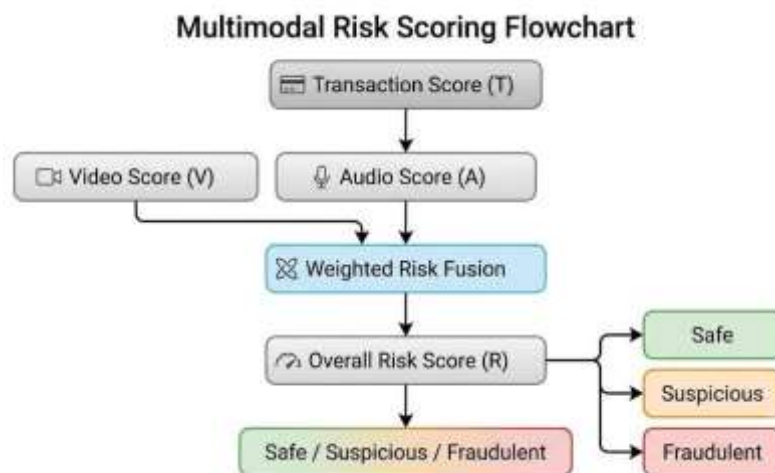
with w_1 , w_2 , and w_3 being weights assigned to each module. One possible weighting system is given below.

Table 3: Example of Module Weighting System

Module	Weight
Transaction	0.45
Audio	0.25
Video	0.30

According to the obtained risk score, the framework will categorize transactions as Safe, Suspicious, and Fraudulent. These thresholds can be defined empirically in the future implementations.

Figure 3: Process of Risk Scoring Using Multiple Modes



12. Post-Quantum Cryptography

In order to increase the security in the long term, our framework proposes using the Post-Quantum Cryptography (PQC) layer for the secure transmission of data. The PQC layer should ensure the following:

- Quantum-resistant key exchange
- Digital signatures
- Secure authentication
- Data integrity
- Confidential communication

The proposed framework recommends using the NIST-approved lattice algorithms like CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures due to the suitability of the algorithm for post-quantum cryptography and secure communications [6, 7]. The hash algorithms like SHA-3 may also be used for the authentication layer [8].

13. Conceptual Processing Algorithm

Algorithm 1: Proposed DeepTrust-UPI Processing Pipeline

Input:

Transaction Details Voice Sample (Optional) Facial Video (Optional)

Output:

Transaction Risk Classification

Step 1: Accept transaction request Step 2: Behavioral anomaly check

Step 3: If risk is above the set threshold, require additional authentication

Step 4: Voice sample analysis for synthetic speech Step 5: Video analysis for deepfake artifacts

Step 6: Multimodal Risk Fusion with analysis results Step 7: Secure communications through PQC

Step 8: Transaction Classification – Safe/Suspicious/Fraudulent End

14. Conceptual Implementation Framework

Because this research suggests the conceptual framework, there is no prototype implementation done in the current research work. The proposed architecture can be considered as reference architecture for future implementations.

During the future implementations, the following technologies like Python, TensorFlow, Scikit-learn, OpenCV, Librosa, and Flask may be used for implementation and validation of the proposed framework. The decision regarding software tools, datasets, and implementation environment may be taken based on implementation goals and computational capabilities.

15. Proposed Workflow

In this way, the proposed framework starts from processing the UPI transaction request. Then, the behavioral analysis of transaction data is done. In case if the transaction is considered risky, further voice and facial verifications are performed. The outputs of transaction analysis module, audio verification module, and video verification module are integrated within the multimodal risk fusion engine to estimate overall fraud risk. The next step is communication protection by Post-Quantum Cryptography layer. As a result of all these processes, the framework gives recommendations about whether the transaction should be accepted or not.

16. Proposed Evaluation Strategy

As the presented framework is the conceptual one, no experiments were carried out in the current research. Thus, the evaluation method which can be used during the future implementation is described in this section.

For the proposed framework, the individual evaluations of transaction anomaly detection module, audio deepfake detection module, and video deepfake detection module as well as overall evaluation of the multimodal risk fusion mechanism can be performed. The framework can be tested using publicly available datasets and simulation scenarios for UPI transactions.

16.1 Evaluation Metrics

In order to evaluate the efficiency of the proposed system, the following performance measures are suggested:

Table 4: Performance Measures for the Proposed System

Metric	Description
Accuracy	Measures the overall correctness of fraud classification.
Precision	Indicates the proportion of detected fraudulent transactions that are actually fraudulent.
Recall	Measures the ability of the framework to identify fraudulent transactions.
F1-Score	Provides a balanced measure of precision and recall.
False Positive Rate	Percentage of legitimate transactions incorrectly identified as fraudulent.
Metric	Description
False Negative Rate	Percentage of fraudulent transactions that remain undetected.
Detection Latency	Time required to analyse and classify a transaction.
Computational Overhead	Processing resources required by the multimodal framework.

Together, these measures offer a comprehensive analysis of detection efficacy and computational efficiency.

16.2 Comparative Analysis

DeepTrust-UPI is an improvement on the existing fraud detection systems by using multimodal artificial intelligence in conjunction with post-quantum cryptography.

Table 5: Comparative Study of Existing and Proposed System

Feature	Conventional UPI Fraud Detection	Proposed DeepTrust-UPI
Transaction Behaviour Analysis	Yes	Yes
Audio Deepfake Detection	No	Yes
Video Deepfake Detection	No	Yes
Multimodal Risk Fusion	No	Yes
Post-Quantum Cryptographic Security	No	Yes

Real-Time Fraud Alerts	Limited	Proposed
Future Quantum Resistance	No	Yes

This proposed framework seeks to improve security during transactions through the combination of behavioral analysis, biometric authentication, and post-quantum cryptography communication under one decision-making architecture.

17. Advantages

The proposed DeepTrust-UPI framework has some strengths over traditional UPI fraud detection systems.

- Combines transaction analysis, voice authentication, and facial verification in one framework.
- Improves the fraud detection process by including multimodal proof rather than using only transaction behavior.
- Uses post-quantum cryptography to provide more secure communication.
- Designs a flexible architecture to support future AI models and improved security.
- Supports intelligent decision making through multimodal risk fusion.
- Is capable of integration with existing systems without the need for replacing the entire system.
- Allows for flexibility for future deployment in real-time financial environment.

18. Limitations

Despite all its potentials, there are a number of weaknesses with the proposed framework.

- This framework is conceptual and has not yet been put into practice or undergone any experimental validation.
- There is a lack of publicly available datasets that include cases of UPI fraud and attacks through deepfakes.
- Multimodal processing can lead to increased computational complexity.
- Implementation in real-time would involve integration with banking systems and regulations.
- Results could be different based on the quality of transactions and multimedia content.

These constraints can serve as an opportunity for implementation and further exploration in the future.

19. Future Scope

The suggested DeepTrust-UPI system can serve as a starting point for future research in intelligent payment security.

Further research can include the development and validation of a working prototype that will use the financial fraud database, deepfake audio data, and facial deepfake data sets. Experimental analysis can be done for the purpose of determining detection efficiency, computational efficiency, and scalability.

Possible future enhancements include:

- Use of real-time UPI payment gateway and banking APIs.
- Use of XAI for transparent fraud detection [5].
- Enhancing federated learning to support privacy-aware model training [12].
- Use of blockchain technology for secure transaction auditing.
- Development of lightweight deep learning models for mobility applications.
- Multilingual voice-based authentication to increase accessibility.
- Behavioral biometrics through continuous behavior analysis.
- Cloud-based implementation for scalability and resilience.

The framework can be upgraded to include future NIST-approved algorithms as post-quantum cryptography standards keep changing to ensure that quantum computing attacks cannot penetrate in the long run.

20. Conclusion

In this paper, we have developed DeepTrust-UPI which is an artificial intelligence based framework to enhance the security of UPI payments against new age cyber attacks. Our framework includes transaction anomaly detection, deepfake audio analysis, deepfake video analysis, and post-quantum cryptography to provide end-to-end security within a single multimodal framework.

Traditional methods of fraud detection are usually based only on transaction behaviour whereas this framework takes a holistic approach by incorporating a variety of authentication methods along with future-ready cryptography. It might be possible that such integration will help in improving fraud detection capability of the model while increasing trust and resilience in digital payment system.

Though this framework has not been implemented or validated experimentally, this paper serves as a strong foundation for future works which might consist of implementing a prototype of this model and testing it with benchmark data sets. It might be possible that such efforts might prove useful for creating intelligent and quantum resistant digital payment systems.

Acknowledgement

The authors would like to thank Assistant Professor Nayana H.P., Department of Computer Science and Business Systems, K.S. School of Engineering and Management for her support and constructive guidance throughout this research.

References

1. Podipireddy A., et al., Multi-Layer UPI Fraud Detection Using Machine Learning, IEEE Conference Publications, 2025.
2. N., Lingareddy, et al., Enhanced Security of Digital Payments through Machine Learning Algorithms, IEEE Xplore Digital Library, 2025.
3. Rani R., et al., Secure UPI: Machine Learning based Fraud Detection System, IEEE Conference Proceedings, 2024.
4. Zhang L., et al., Anomaly detection through Isolation Forest Algorithm, IEEE Access, 2022.

<https://doi.org/10.1109/ACCESS.2022.3145678>

5. A., Khot, et al., Multimodal Financial Fraud Detection System Using Explainable Artificial Intelligence, IJFMR Journal Publications, 2025.
6. Bavdekar R., et
7. Chandre P., et al., Post Quantum Cryptography in Critical Infrastructures, IEEE International Conference Proceedings, 2024.
8. Sha 3 For FPGA Based Multimodal Biometric Authentication, Sravani M.M., et al., IEEE Transactions,
9. Goodfellow, I., et al. Generative Adversarial Nets. In Advances in Neural Information Processing Systems (NeurIPS). 201
10. Vaswani A., et al. Attention is All You Need. Advances in Neural Information Processing Systems (NeurIPS), 2017. <https://arxiv>
11. OpenAI. GPT-4 Technical Report. OpenAI Research, 2
12. I. H. Sarker, Machine Learning: Algorithms, Real World Applications and Future Research Directions, SN Computer Science, 2021.