International Research Journal of Multidiciplinary Sciences (IRJMS) Issue 5, Volume 2,PP 1-12,
Double Blind Peer Reviewed ISSN 3107-930X(ONLINE)

SecureAI-UPI: A Multi-Layer Authentication Framework for Securing Voice-Enabled UPI Transactions Against Deepfake and Voice Cloning Attacks

[1]ABHINEET KUMAR VISHWAKARMA
Amity Institute of Information Technology
Amity University Lucknow Campus
Lucknow, Uttar Pradesh, India
abhineet.vishwakarma@s.amity.edu

[2]DR. UMAR KHALID FAROOQUI
Assistant Professor
Amity Institute of Information Technology
Amity University Lucknow Campus Lucknow,
Uttar Pradesh, India
ukfarooqui@amity.edu

Abstract: **The Unified Payments Interface (UPI) has revolutionized India's digital payments landscape with its secure, real-time, and hassle-free financial transactions. But new developments in generative artificial intelligence have added sophisticated cyber threats, such as Deepfake and voice cloning attacks, that can be used to commit identity theft, social engineering and financial fraud. Conventionally used UPI systems use binding devices, securecommunication, and UPI PIN validation as key approaches to ensure proper authentication. However, voice-based payments via UPI, such as NPCI's Hello UPI, conversation banking, and AI chatbots provide a new attack vector which can be used against them via the use of Deepfakes and AI clones of the voice. Instead of creating another approach to UPI authentication and replacing the existing methods, it is proposed to use a complementary approach called SecureAI-UPI. This paper explores the security threat that can be created due to Deepfake an voice cloning technologies in UPI authentication systems and the inadequacies of the existing authenticationmechanisms.Tomitigatethem,we propose the concept of a multi-layer authentication system SecureAI-UPI, combining device trust evaluation,behavioral biometrics, liveness detection on the speaker's voice, analysis of the risk of the transaction, contextual risk analysis, and adaptive multi-factor authentication. The proposed framework has a multi-layered intelligent approach for security that aims to resist AI-based impersonationattacks,while ensuring compatibility with the current UPI infrastructure. A comparative security analysis is used to illustrate how SecureAI-UPI can better address issues of fraud detection than traditional authentication methods and design a pragmatic defensive strategy that enhances fraud detection while minimizing additional user interactionthroughadaptive risk-basedauthentication.]**

Keywords:Unified Payments Interface (UPI), Deepfake Detection, Voice Cloning, Digital Payment Security, Behavioral Biometrics, Adaptive Authentication, Artificial Intelligence, Financial Fraud.

III. INTRODUCTION

Unified Payments Interface (UPI) has revolutionized India's digital payment landscape by helping instant, interoperable, and secure financial transactions via mobile devices [1], [2]. Created by the National Payments Corporation of India (NPCI), UPI is now among the world's most successful real-time payment services processing billions of transactions each month [1]. It has greatly facilitated financial inclusion, made peer-to-peer and merchant payments easier, and improved India's digital economy. Unfortunately, increasing numbers of transactions also create a larger attack surface for cybercriminals that see UPI as a new lucrative target of fraud attacks. Modern development of Generative Artificial Intelligence (GenAI) tools has significantly raised the level of complexity of cyber threats [3], [4], [6]. Thanks to such technologies as Deepfake and voice cloning, cybercriminals can produce synthetic voices and visual content that can accurately impersonate a user of a legitimate account. These technologies were initially used in media generation and accessibility purposes, but now they are increasingly employed to perform social engineering attacks, deceptive customer service operations, impersonation of identities, and even financial frauds. Open-source AI models and cloud-based voice synthesis services have also helped

cybercriminals to lower the threshold for AI-powered fraud [3], [6]. UPI applications like Google Pay, PhonePe, and Paytm currently utilize methods like device binding, cryptographically secured communication channels, and UPI PIN for authentication, which ensure a good level of security from all conventional attacks. Recently, NPCI came up with Hello UPI and similar conversational payment systems where individuals can make their financial transactions using voice-based interfaces. Although these innovations have added ease of access for users, they come with a potential vulnerability as well, since AI-generated voices and voice cloning systems can mimic authentic users with high accuracy. Hence, there is a need for future voice-based payment systems to authenticate voices of actual humans from those of AI without affecting current UPI authentication procedures. In such cases, cyber criminals may exploit artificial intelligence-based cloning of voices to fool users, bypass voice authentication process, and authorize illegitimate transactions using social engineering techniques. As AI media becomes more realistic, traditional authentication methods can prove to be insufficient to detect AI-based impersonations. This is because to protect from the above threats that are emerging, this paper recommends the development of SecureAI-UPI, which is a multi-tier authentication solution aimed at securing both existing and new voice-based payment systems from AI-enabled unlike traditional systems, which depend on a limited number of verification methods, the proposed framework combines behavioral biometric recognition, device trust analysis, voice liveness detection, transaction analysis, and adaptive multi-factor authentication. The system will complement UPI authentication rather than replace any of its components and add intelligent verification layers to detect anomalous user behavior and impersonations performed via artificial intelligence. Purpose: The purpose of this research is to evaluate the security threats due to Deepfake technology and voice cloning techniques in the UPI ecosystem, explore flaws in existing authentication techniques, and design a pragmatic defensive strategy that proves fraud detection without compromising usability. The research paper will also explore various implementation issues and privacy concerns related to securing AI-based digital payments systems from cyber threats.

A. Research Gap

While extensive work has been done on each of these aspects of UPI security, biometric authentication, Deepfake detection, and voice cloning, these have been largely developed as separate research areas. [1], [10] The current security measures used in UPI are mainly to secure payment systems using device binding, PIN verification, biometric verification and transaction monitoring. Likewise, studies on Deepfake and voice cloning have focused primarily on detecting these attacks and creating media forensics tools, rather than real-time financial authentication systems. [3], [5], [6] Current approaches to user authentication assume that the biometric/voice data is generated by a real person. Traditional uses of UPI technologies use PIN authentication methods, while conversational payments and voice-banking systems need some extra security measures to prevent deep-fake and synthetic speech attacks. [10] Furthermore, current fraud detection tools tend to focus on transaction behavior without incorporating behavioral biometrics, device trust evaluation, voice liveness detection, contextual risk analysis, and adaptive authentication within a single decision-making flow. [13], [15]

Though substantial work has been done on the topics of security in UPI transactions, biometric authentication, and Deepfake audio, there is little work done on combining these topics together in order to secure upcoming voice-enabled UPI platforms. The current framework has been developed mainly for use in PIN-based mobile payment platforms; thus, it does not take into account AI-based voice impersonation attacks that might be launched against such platforms. To address this, this paper presents SecureAI-UPI, an integrated authentication framework that uses multiple complementary security mechanisms to enhance fraud resiliency and is compatible with the existing UPI infrastructure. [17], [18]

B. Research Contributions

Threat Analysis: Comprehensive analysis of AI-generated deepfake and voice cloning attacks targeting voice-enabled UPI services, conversational payment platforms, and customer authentication workflows. [3], [5], [6]
Threat Modeling: Creation of a systematic threat model that explains how AI-assisted impersonation threats can exploit weaknesses in current authentication processes. [12] SecureAI-UPI Approach: A proposed concept of multi-layer authentication framework that combines device trust evaluation, behavioral biometrics, conditional voice liveness detection for voice-enabled payment service, contextual transaction risk analysis, and adaptive multi-factor authentication. [10], [13], [17]
Security Analysis: Comparative analysis explaining how the suggested approach resolves limitations in traditional authentication schemes to counter AI-based threats.
Future Research Directions: Exploration of implementation challenges, privacy concerns, computational aspects, and future scope of AI in securing digital payment platforms.

IV. RELATED WORK

Recent advancements in the security of digital payments have been achieved through biometric authentication, fraud detection, and AI-basedsecurity systems [4], [5], [6],[15].Nevertheless,thedevelopmentofDeepfakeand voice cloning technology poses a new form ofimpersonation attack against the security systems of digital payment. Presently, most researchers are interested indeveloping either improvedauthenticationofdigitalpaymentsordetection,and no research integrates both concepts to secure UPI transactions. Some researchers havesuggested methods of improving user authentication in UPI systems by using biometric verification and deep learning models [4]. These techniques enhance user authentication but assume that the input biometric features belong to valid users without considering thepossibility of AI-generated synthetic voices. In addition, some current research on audio Deepfake detection has shown high performances usingtransformers, spectral features analysis, and challenge-response systems[3], [5], [6]. Even though these techniques effectively classify genuinespeech from the synthetic one, their applications are more focused on thestandalone voice authentication systems than the digital paymentinfrastructure. Recent surveys have also emphasized the growingtrendstowardsusingbehavioral biometrics, contextual risk analysis, and adaptive authentication for increasing the security level of financial transactions[13]– [15]. However, such measures are usually performed in isolation without any unified system for analyzing device trustworthiness,user behavior, transaction context,andfakeuserscreatedwiththehelpofAItechnology during the process of authenticating the UPI transaction.The key challenge in this regard is that the current research lacks an integrated security system specifically tailored todefending the UPIenvironment from AI-enabled Deepfakes and voice-cloning attacks. This paper fills the gap by presenting a secure authentication framework, called SecureAI-UPI.

Table I highlights a comparison between the various methods adopted to protect thedigital payment system fromthreats using artificialintelligence(AI).Eventhoughseveralresearchprojects have been conducted previously to strengthen the security of digital payment systems by incorporating authentication techniques such as biometric authentication, voice verification, and behavioral recognition, none of the methods have incorporated all these techniques.

Study	Focus	Limitation
UPI Authentication Models	PIN,biometrics, device verification	Limitedprotectionagainst AI-driven impersonation
Voice Authentication Systems	Speaker verificationusing voice biometrics	Vulnerable to high-qualityvoice cloning
AudioDeepfake Detection	Detection of syntheticspeech	Notintegrated with UPI transaction workflows
Behavioral Authentication	Continuoususer behavioranalysis	Doesnotverify. AI-generated voiceattacks
Proposed SecureAI-UPI	Multi-layerAI-assisted UPI authentication	Integrates behavioral, contextual,and AI-based verificationfor improved fraud. resilience

TableI.ComparisonofExistingApproaches

V. THREAT MODEL AND UPI AUTHENTICATION ANALYSIS

UPIusesalayeredapproachtoauthenticatetransactionsthat include device binding, user authentication, encryption of communications,andUPIPIN[1],[10].Ineachtransaction, device authentication is done by device registration of the user's mobile phone, followed by secured communication with the issuer and acquirer banks by the NPCI. Finally, transaction authentication is done using the UPI PIN or biometrics

depending on the application. Although this model provides adequate security against conventional threats such as phishing, harvesting credentials, and unauthenticated device access, itisnotprotected fromAI-based attacks exploiting human trust.

Generative AI has significantly improved the effectiveness of Deepfake and voice cloning tools [3], [5], [6]. These attackers can produce highly authentic synthesized voices in just a few seconds of publicly accessible voice recordings. With this capability, these attackers can pretend to be the legitimate user during customer service calls and other social engineering schemes. Instead of stealing passwords or cryptographic keys like in traditional attacks, attackers manipulate humans to authorize transactions or provide their authenticating credentials. To methodically identifythese threats, the research uses the STRIDE Threat Modelingtechnique.IntheSTRIDEmodel,therearesix categories of threats – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [12]. Out of these, Spoofingis one of the most severe threats in cases of AI-based UPI fraud, in which attackers employfake or spoofed voices for posing as genuine users. There can be instances of Information Disclosure through social engineering. using AI, as well as cases of Elevation of Privilege through spoofing or compromised authentication.

Threat Category	**ExampleinUPI**	**Proposed Mitigation**
Spoofing	AI-generated voice impersonation	Voiceliveness detection + Behavioral biometrics
Tampering	QR code or transaction modification	End-to-end encryptionand integrity verification
Repudiation	Denial of performed transactions	Secureaudit logging and digitalsignatures
Information Disclosure	Socialengineering using Deepfake voices	Adaptive authenticationand user verification
Denial of Service	Authentication requestflooding	Rate limiting and anomalydetection
Elevatio n of Privilege	Unauthorized account access	Devicetrust scoring and adaptiveMFA

TableII.STRIDE-BasedThreatAnalysisforUPI Authentication

Table II provides a summary of the different security threats met during the process of UPI authentication by usingtheSTRIDEmodelandmatchingeachoneofthemwith its respective defense measures. It can be seen that traditional forms of authentication can only protect from technical attacks while providing negligible security against any kind of impersonation and behavior modification by the use of AI.

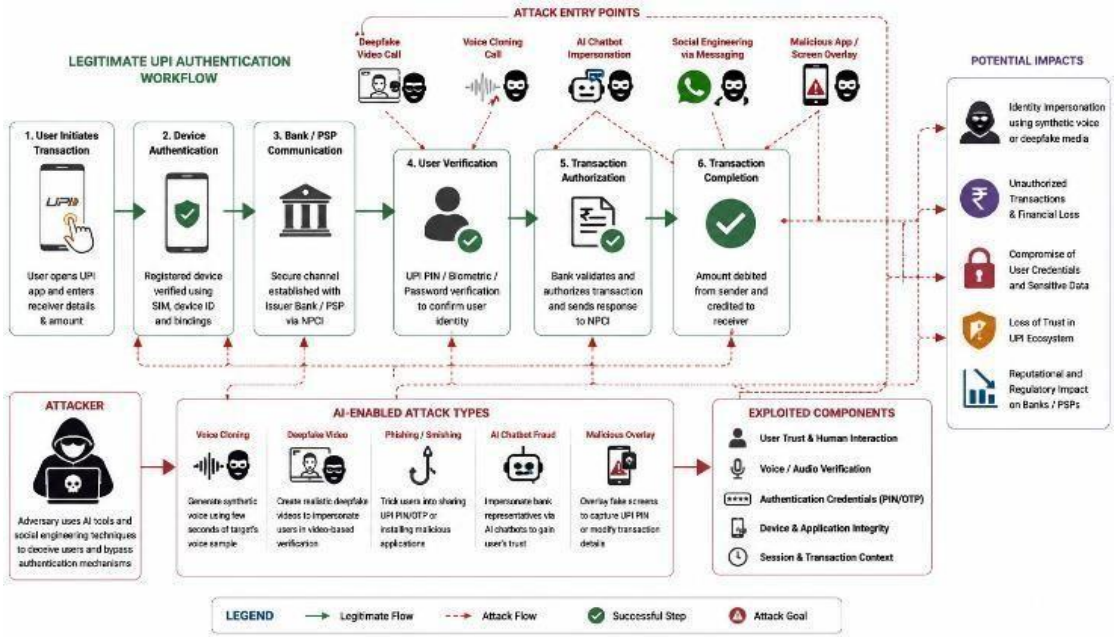

Fig.1.ThreatmodelillustratingAI-enabledDeepfake and voice-cloning attacks against the UPI authentication workflow.

VI. Proposed SecureAI-UPI Framework

To prevent potential impersonation attacks enabled by AI, SecureAI-UPI framework is suggested in this research work to enhance thesecurityofUPI transactions byimprovingthe current authentication process without changing the existing authentication setup. [1], [10] Unlike traditional static authentication factors that include device binding, UPI PIN authentication, or biometric authentication, the framework evaluates several factors for security prior to authenticating any transaction. The purpose of implementing thisframeworkisto findanysuspiciousbehaviorandfake media attacks while providing seamless user experience to legitimateusers. [17]There are five distinct security layers within theproposed framework. TheDeviceTrustModuleis used to verify the authenticity of the registered device through various means such as device fingerprinting, SIM binding, OS integrity check, and app verification [10], [12].It will ensure that only legitimate devices are used for sensitive transactions. The second module is the Behavioral Biometrics Module where continuous behavioral analysis is performed for different user interaction patterns like typing speed, touchdynamics, swipingpattern, transaction rate,and location [13], [15]. The third layer conducts Voice Liveness and Deepfake Detection in case there is anyinvolvement of voice-based verification or interaction with the customer. Rather than processing the voice input, the framework processes liveness factors, spectral discrepancies, replay detection, and artificial speech recognition to separate genuine users from voice fakes made by AI [17], [18]. The fourth layer is used for Transaction Risk Analysis, where information about the context of the transaction is gatheredto assess the possibility of a fraud, including transaction amount,transactionrecipient,devicereputation,geolocation, and transaction timing. Finally, the Adaptive Authentication Engine aggregates the results of all the earlier modules to decide the total transactionrisklevel[10],[17].Transactions with a minimal risk level are allowed without any special actions, while transactions at a medium risk level should be verified via biometrics or one-time

password. Transactions thatareconsideredelevatedriskaresuspendedandedirectedforfurtherreviewforfraudanalysis.Thedesign will provide the UPI system with an improved versionof the current authentication mechanism byincorporatingseveralindependentparametersto create a single decision-making framework. Even if one of the authentication parameters is compromised, the rest will keep verifying the validity of the transactions.

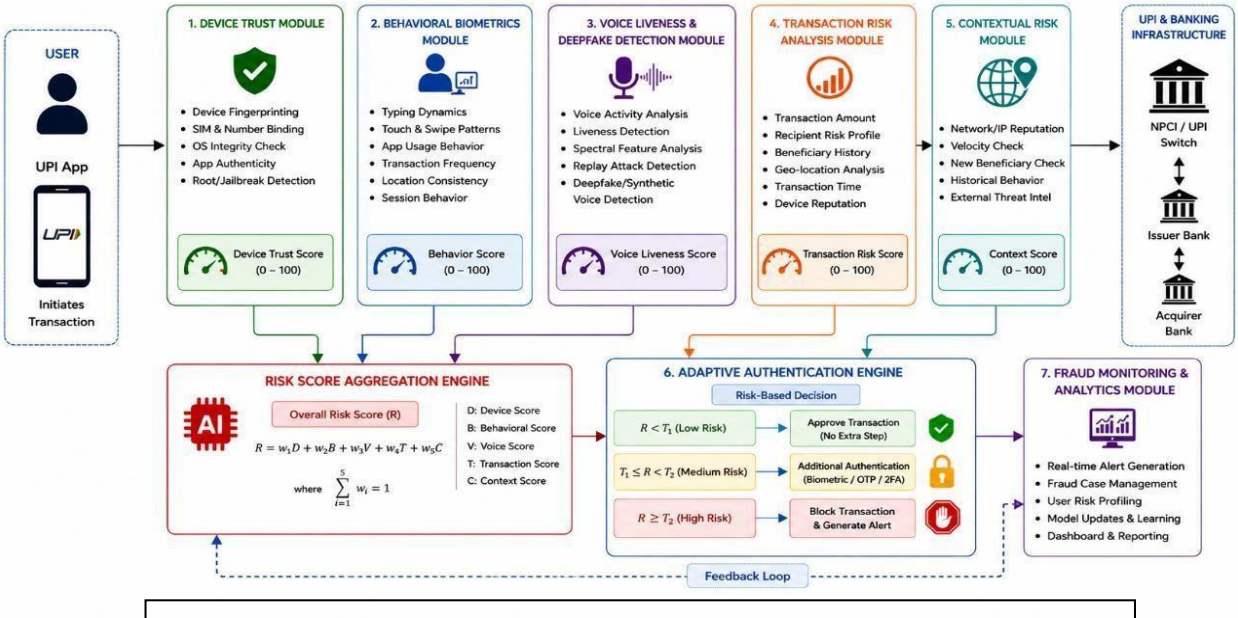

Fig.2.ArchitectureoftheproposedSecureAI-UPImulti-layerauthenticationframework.

V. Security Evaluation and Discussion

The proposed SecureAI-UPI solution was analyzed comparativelyfor its securityagainst the traditional UPI authentication scheme. Unlike the use of only one authentication mechanism, the SecureAI-UPI solution combines several layers of security, which includes the following – device trust evaluation, behavioral biometrics, voice liveness detection, transaction risk analysis, and adaptive multi-factor authentication. Traditional UPI authentication is based on device binding, UPI PIN authentication, and biometric authentication. These traditional schemes ensure strong protection against credential stealing and unauthorized access to devices [1], [10]. However, these schemeshave no effective defense against advanced attacks with the help of Deepfake media content, artificial speech, andAI-poweredsocialengineering[3],[5],[6].Withthe inclusion of contextual and behavioral analysis, the proposed framework will allow finding unusual transaction patterns. [13], [15] In addition, adaptive authentication decreases the number of authentications performed unnecessarily for valid users and increasesthe security in case of risky transactions. As opposed to the uniform application of authentication criteria in all transactions,theSecureAI-UPIframework makesuseof transaction risk scores in order to adapt verification accordingly. [10], [17]

While the proposed architecture is quite promising, the practical implementation of such a solution depends on thedevelopmentofAImodelsthatperforminferencefast and have low computational cost. [17], [18] There are some other factors to consider prior to practical implementation of the framework.

Table III provides a comparative analysis of the proposed SecureAI-UPI framework versus traditional approaches for verifying a user's identity through UPI. From the table, itcan be seen that

while existing frameworks mostly focus on static forms of verification, the framework introduced by SecureAI-UPI offers intelligent risk-based layers for identification of AI-driven impersonations.

SecurityFeature	Conventional UPI	SecureAI-UPI
DeviceAuthentication	✓	✓
UPIPINVerification	✓	✓
BehavioralBiometrics	✗	✓
VoiceLivenessDetection	✗	✓
DeepfakeDetection	✗	✓
TransactionRiskScoring	Limited	✓
AdaptiveAuthentication	✗	✓

VI. Computational Efficiency and Latency Optimization

The key feature of Unified Payments Interface (UPI) is to completetransactionswithinafewseconds,withmoneyusually authorized as soon as the transaction is done. [1], [10] Hence, any extra authentication procedure should yield more security without undue processing time delay. [17]

The proposed SecureAI-UPI framework is different from the traditional sequential authentication system that uses a linear architecture. The SecureAI-UPI framework proposed in this paper is a risk adaptive and parallel processing architecture. Only the security mechanism(s) required for the level ofsecurity needed for the transaction are activated, rather than executing all security modules for all transactions.

A. ParallelAuthenticationArchitecture

he system has multiple lightweight authenticationmodules running concurrently in transaction processing.

Theseinclude:

1. DeviceTrust Evaluation
2. BehavioralBiometricsMonitoring
3. TransactionMetadata Analysis

Being executed sequentially, these modules share the execution time resulting in a shorter overall authentication delay.

B. SelectiveVoiceAuthentication

VoiceLivenessDetectionisnotrunduringallUPI transactions.

Themodulewillonlybeactivatedifthetransactionincludes:

1. NPCIHello UPI
2. Voice-assistedbanking
3. Conversationalpaymentsystems
4. AI-poweredfinancialassistants

The traditional UPI apps, which do not require voice verification, are still in use. This selective activationreduces number of computations while maintaining compatibility with the existing UPI ecosystem.

C. Risk-AdaptiveAuthentication

The proposed framework applies different security checks per transaction based on the risk of the transaction

rather than applying the same security checks for all transactions.

TransactionRisk	AuthenticationProcess
Low Risk	DeviceTrust+PIN
MediumRisk	DeviceTrust+Behavioral Analysis+AdaptiveMFA
HighRisk	DeviceTrust+Behavioral Biometrics + Voice Liveness (if applicable) + TransactionRisk Analysis +ManualFraud Review

Thisadaptivestrategydecreases theamountofcomputation required for valid transactions, and only allocates extra computation for suspicious transactions.

D. EdgeAIProcessing

Where possible, modules that require a lot of computation are performed on the user's device to further minimize latency and preserve user privacy. [17], [18]

Examplesinclude:

1. Deviceintegrity verification
2. Behavioralbiometricanalysis
3. Voicelivenessinference

Anonymizedauthenticationscoresareonlysenttothe centralriskassessmentengine,lesseningnetwork

VII. Privacy-Preserving Framework Design

Although behavioral biometrics, contextual analysis, and voice liveness detection greatly increase the level of security in the authentication process, they also raise privacy concerns due to their need for ongoing monitoring of user interactions. To comply with privacy principles of today, the proposedSecureAI-UPI architecture follows a principle of "privacy by design," with the processing of sensitive biometric information being done locally on the user's device whenever possible,DSPs that leverage AI are considered

A. EdgeAI-BasedProcessing.

Lightweight on-device machine learning models are used to perform behavioral biometric analysis, device trust verification, and voice liveness detection. No raw biometric data, like touch dynamics, typing patterns, voice recordings or sensor information is sent to centralized servers. Instead, only anonymized authentication confidence scores are passed on to the central risk assessment engine. It decreases the latency of communications and the exposure of sensitive biometric data.

B. FederatedLearning

SecureAI-UPI future implementations could use Federated Learning to continuously enhance the authentication models without having to collect users' raw personal data. [17], [18]

Underthis approach:

1. Alluser data isstoredonthedevice.
2. Onlyencryptedmodelupdatesare sent.
3. Thecentralservercollectstheparametersofthemodels.

4. Noindividualbiometricdataeverleavesauser'ssmartphone!

This dramatically lowers threatsto privacy, andimproves and refines the model continuously.

C. SecureDataProtection

It is assumed that all communication between the mobile application, banking servers, and the NPCI infrastructure has strong cryptographic protection namely: [8], [16]

1. End-to-End Encryption
2. TLS1.3SecureCommunication
3. AES-256Data Encryption
4. SecureKeyManagement
5. DigitalSignatures:Integrityof Transactions

These mechanisms safeguard the integrity of authentication information during transaction processing against interception, modification and unauthorized disclosure.

D. DataMinimization

The framework is based on the concept of data minimization – only the necessary data for authentication is processed. [17]

Examplesinclude:

1. Authenticationconfidence score
2. Deviceintegritystatus
3. Behavioralanomalyscore
4. Transactionrisk score

Sensitive data like complete voice recordings, continuous typing logs or raw touch traces are not stored permanently but are discarded immediately following local processing.

E. PrivacyBenefits

Theproposed architecturehasanumberof advantages:

1. Safeguardingofvulnerablebiometric data.
2. Decreasedriskofcentralizeddatabreaches.
3. Reducenetworkbandwidthusage.
4. Quickauthenticationvialocalinference.
5. Increased adherencetonewprivacy laws.

SecureAI-UPI is a federated learning model which combines Edge AI with encrypted communication and data minimization, to boost authentication security whilekeeping user privacy and lowering computational costs. [17],[18]

VIII. Prototype Implementation and Future Validation

The SecureAI-UPI model described in this paper is at present considered as a conceptual security architecture model that would illustrate the viability of combining various authentication approaches in securing emerging voice-based UPI services from AI-based impersonation attacks. [10], [17] The current section does not discuss any results of experiments, but instead, provides a systematic approach to future implementation and evaluation.

The model will be developed as a modular authentication system based on various security modules connected to each other through a centralized risk assessment engine. Each module will perform specific security functions while simultaneously providing its confidence score to the adaptive decision engine.

- The implementation will include the following components:

1. Device Trust Module
i) Device fingerprinting
ii) SIM binding check
iii) Root/Jailbreak detection
iv) Application integrity check

2. Behavioral Biometrics Module
i) Touch dynamics
ii) Swipe behavior
iii) Typing rhythms
iv) Transaction frequency
v) Interaction patterns of the device

3. Voice Liveness and Deepfake Detection Module
i) Analysis of spectral features
ii) Detection of replay attacks
iii) Detection of synthetic voices
iv) Challenge-response verification
v) Speaker liveness assessment

4. Transaction Risk Analysis Module
i) Transaction amount
ii) Beneficiary history
iii) Device reputation
iv) Location consistency
v) Time of day analysis

5. Adaptive Authentication Engine
i) Risk aggregation
ii) Decision making
iii) Step-up authentication
iv) Fraud alerts

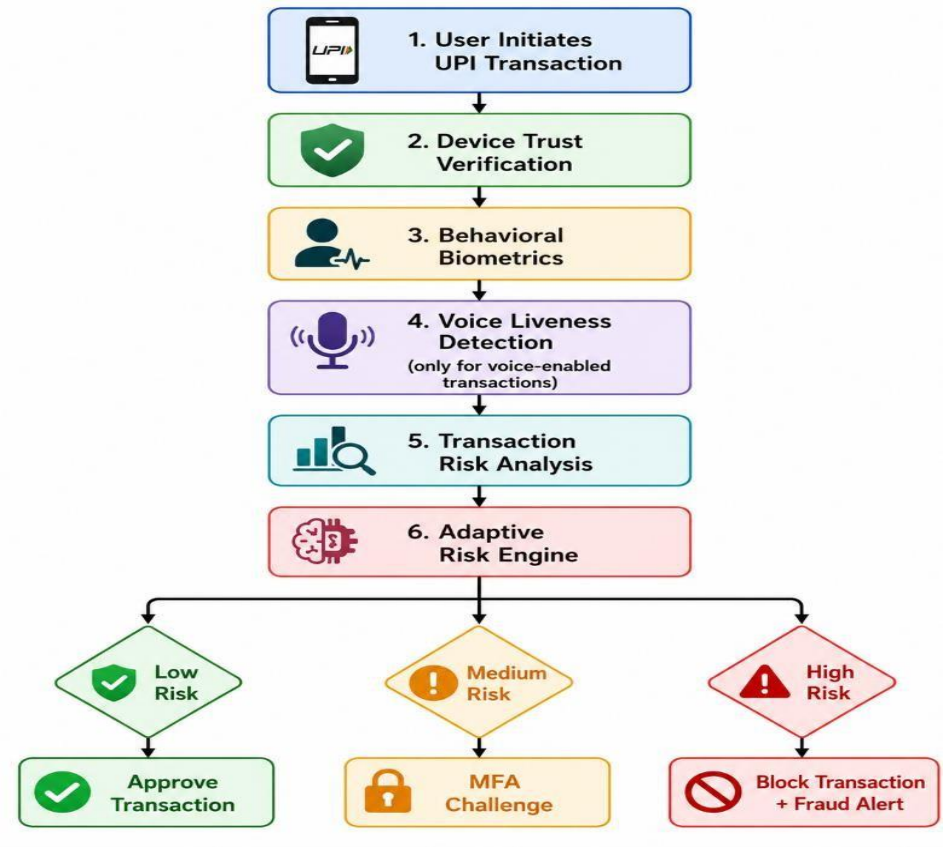

Fig.3 Prototype Workflow

IX. Conclusion

The rapid development of technologies such as Deepfake and voice cloning raises serious issues related to the security of contemporary digital payment systems [3], [6]. Even though contemporary mechanisms of UPI authentication ensure reliable security against traditional cyber-attacks, these technologies do notincludemeasuresintended toprotectagainstattacksbased onAI technology that utilizes people's trust and context-based vulnerabilities. SecureAI-UPI is a concept of a multi-layer authentication framework that includes such components as trust evaluation for devices, behavioral biometrics, voice liveness detection, transaction risk assessment, and adaptive multi-factor authentication. Comparative Security Analysis and Discussion of the proposed model demonstrate its capabilityofenhancingsecurityagainstattacksdrivenbyAI technology without compromising the usability and effectiveness of UPI system [1], [10].'

In future works, our efforts will be concentrated towards development and validation of the entire system by using benchmark data sets such as AS spoof for the detection of voice spoofing and behavioral biometric databases for continuous verification of the user identity. [3], [5], [6] The system will be confirmed through well-known security parameters such as FAR, FRR, EER, precision, recall, F1-score, authentication latency, and computationalcomplexity.communicationoverheadandresponsetime.

X. References

[1] *National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI)," 2025. [Online].*

[2] *Reserve Bank of India, Annual Report 2024–25, Mumbai, India, 2025.*

[3] *N. Jiang, Z. Wang, et al., "Foice: Face-to-Voice Deepfake AttackonVoiceAuthenticationSystems,"inProc. 33rd USENIX Security Symposium, 2024.*

[4] *P. Khekare, A. Patil, and S. Sharma, "Deep Learning-Based Voice Authentication forSecure UPI Transactions,"International Journal of Intelligent Systems and ApplicationsinEngineering,vol.12,no.5,pp.1023–1034, 2024.*

[5] *S. Mittal et al., "PITCH: Detecting Real-Time Audio Deepfakes Using Challenge-Response Verification," arXiv:2402.18085, 2024.*

[6] *Y. Liu, X. Zhang, and H. Li, "A Survey on Audio Deepfake Detection Using Deep Learning," Sensors, vol.25, no. 7, 2025.*

[7] *R.Anderson,SecurityEngineering,3rded.Wiley,2020.*

[8] *W.Stallings,CryptographyandNetworkSecurity: Principles and Practice, 8th ed. Pearson, 2023.*

[9] *B.Schneier,AppliedCryptography,20thAnniversary ed. Wiley, 2015.*

[10] *NationalInstituteofStandardsandTechnology (NIST), Digital Identity Guidelines (SP 800-63B), 2024.*

[11] *MITRE Corporation, "MITRE ATT&CK Framework," 2025.*

[12] *Microsoft,"ThreatModelingUsingSTRIDE," Microsoft Security Documentation, 2024.*

[13] *A.K.Jain,A.Ross,andK.Nandakumar,*Introduction to Biometrics,*2011*