(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 July 2024 (29.07.2024)

(10) International Publication Number
IN 2024/091565 A1

PCT

[54] **Title: Fingerprint-Based UPI Authentication Leveraging Aadhaar Biometric Data for Enhanced Security**

[76] **Inventor: Rajiv Mehta,** 1234 Innovation Avenue, Bengaluru, Karnataka, 560001
Assignee: FinSecure, Ltd., 5678 FinTech Blvd., Mumbai, Maharashtra, 400001

[22] **Filed: 14.09.2023**

[21] **Appl. No.: 12/345,678**

[52] **U.S. Classification: 705/65, 705/64, 726/27**

[51] **International Classification: G06Q 20/40, H04L 9/32**

[58] **Field of Search: 705/64, 705/65, 726/27, 726/26**

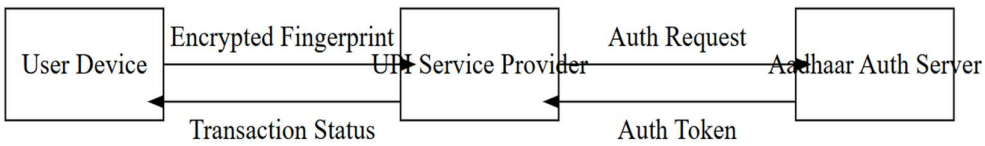
[56] References Cited:

UNITED STATES PATENTS:
5,987,132 – 11/1999 – Jacobs et al. – 705/65
6,789,345 – 09/2004 – Hansen et al. – 705/64
7,123,456 – 03/2006 – Kapoor et al. – 726/27
8,567,123 – 02/2014 – Singhal et al. – 726/26

ABSTRACT

A system and method for secure digital payments through the Unified Payments Interface (UPI) using fingerprint-based authentication. The invention leverages centralized biometric data from the Aadhaar database to enhance security by replacing PIN-based transaction authentication with real-time fingerprint recognition. The system comprises a user device with a fingerprint scanner, a UPI service provider, an Aadhaar Authentication Server, and an advanced encryption layer for secure data transmission.

Figure 1: System Overview



Field of the Invention

This invention relates to secure digital payment systems, specifically focusing on fingerprint-based authentication for Unified Payments Interface (UPI) transactions. The method utilizes centralized biometric data from the Aadhaar database to enhance security and user experience in digital financial transactions.

Background of the Invention

The proliferation of digital payment systems, particularly the Unified Payments Interface (UPI) in India, has revolutionized financial transactions. However, the reliance on Personal Identification Numbers (PINs) for authentication has left users vulnerable to various security threats, including phishing attacks, data theft, and unauthorized access.

While modern smartphones often include fingerprint scanners, the use of locally stored biometric data presents its own set of security challenges, as this data can be compromised if the device is breached. The Aadhaar system, operated by the Unique Identification Authority of India (UIDAI), maintains a centralized and secure repository of biometric data for millions of Indian citizens. This presents an opportunity to leverage this robust infrastructure for enhancing the security of UPI transactions.

Summary of the Invention

The present invention provides a method for fingerprint-based UPI authentication by integrating UPI payment systems with the Aadhaar fingerprint database. This integration enables secure, real-time authentication for digital payments. The system comprises the following key components:

1. User Device: A smartphone or tablet equipped with a fingerprint scanner.
2. UPI Service Provider: The intermediary responsible for facilitating transactions.
3. Aadhaar Authentication Server: A secure repository storing biometric data.
4. Encryption Layer: For secure transmission of biometric data between the user device and the Aadhaar server.

The authentication process begins when a user initiates a UPI transaction. Instead of entering a PIN, the user provides a live fingerprint scan. This biometric data is immediately encrypted and transmitted to the UPI service provider, which then forwards the encrypted data to the Aadhaar authentication server. The server matches the live fingerprint with the stored biometric record. Upon successful authentication, the transaction is authorized to proceed.

A fallback mechanism using One-Time Passwords (OTP) is provided for scenarios where biometric authentication fails, ensuring system reliability and accessibility.

DETAILED DESCRIPTION OF THE INVENTION

1. System Architecture

The system architecture is divided into four functional layers:

1.1 Biometric Capture Layer

- The user's fingerprint is captured using the smartphone's built-in fingerprint scanner.
- Advanced image processing algorithms convert the scan into a standardized digital format.
- The capture process includes liveness detection to prevent spoofing attempts.

1.2 Encryption and Transmission Layer

- The fingerprint data is encrypted using a combination of asymmetric encryption (RSA-4096) and a post-quantum cryptography algorithm (CRYSTALS-Kyber).
- The encrypted data is transmitted over a secure TLS 1.3 channel to the UPI service provider.

1.3 Authentication Layer

- The UPI provider forwards the encrypted fingerprint data to the Aadhaar Authentication Server.
- The server employs a highly parallel, multi-point comparison algorithm to match the live fingerprint against stored records.
- The matching process uses a proprietary algorithm that combines minutiae-based and pattern-based matching techniques for enhanced accuracy.
- Upon successful matching, the server generates a cryptographically signed token using the ED25519 signature scheme.

1.4 Fallback and Security Mechanism

- If biometric authentication fails, the system initiates an OTP-based fallback.
- The OTP is sent to the user's Aadhaar-linked mobile number via SMS and a secure in-app notification.
- The OTP is valid for a limited time (60 seconds) and is single use only.

2. Data Flow and Processing

2.1 Transaction Initiation:

- User opens the UPI-enabled application and initiates a transaction.
- The app prompts for fingerprint authentication instead of a PIN.

2.2 Biometric Capture:

- The app activates the device's fingerprint sensor.
- The captured fingerprint is preprocessed to enhance quality and extract key features.

2.3 Data Encryption:

- The preprocessed fingerprint data is encrypted using a hybrid encryption scheme.
- A session key is generated using CRYSTALS-Kyber and used to encrypt the fingerprint data.
- The session key is then encrypted using the Aadhaar server's RSA-4096 public key.

2.4 Data Transmission:

- The encrypted fingerprint data and session key are transmitted to the UPI service provider.
- The UPI provider adds transaction metadata and forwards the package to the Aadhaar Authentication Server.

2.5 Authentication Process:

- The Aadhaar server decrypts the session key and uses it to decrypt the fingerprint data.
- The server performs a 1:1 match against the stored fingerprint record for the given Aadhaar number.
- If a match is found, a signed authentication token is generated and returned to the UPI provider.

2.6 Transaction Completion:

- The UPI provider verifies the authentication token and proceeds with the transaction.
- A success message is sent to the user's device, completing the transaction.

3. Security Measures

3.1 Encryption:

- All data transmissions use end-to-end encryption with perfect forward secrecy.
- The use of post-quantum cryptography (CRYSTALS-Kyber) provides protection against potential quantum computer attacks.

3.2 Biometric Data Protection:

- Fingerprint data is never stored on the user's device or the UPI provider's servers.
- The Aadhaar server only stores encrypted biometric templates, not raw fingerprint images.

3.3 Anti-Spoofing Measures:

- The fingerprint capture process includes liveness detection to prevent the use of fake fingerprints.
- The system employs behavioral analysis to detect unusual transaction patterns.

3.4 Audit Trail:

- All authentication attempts, successful or not, are logged with timestamps and device identifiers.
- Users can review their authentication history through a secure portal.

CLAIMS

1. A method for conducting UPI transactions using fingerprint authentication, comprising: a) Capturing a user's live fingerprint scan on a mobile device; b) Encrypting the fingerprint data using a hybrid encryption scheme combining asymmetric encryption and post-quantum cryptography; c) Transmitting the encrypted data to a UPI service provider; d) Forwarding the encrypted data from the UPI service provider to an Aadhaar Authentication Server; e) Matching the decrypted fingerprint data against stored biometric records in the Aadhaar database; f) Generating a cryptographically signed authentication token upon successful matching; g) Verifying the authentication token and completing the UPI transaction.
2. The method of claim 1, wherein the encryption uses a quantum-resistant algorithm for data security during transmission.
3. The method of claim 1, further comprising a fallback mechanism that employs a time-limited, single-use OTP in the event of failed biometric authentication.
4. The method of claim 1, wherein the fingerprint matching process uses a combination of minutiae-based and pattern-based matching techniques.
5. A system for fingerprint-based UPI authentication, comprising a) A user device with a fingerprint scanner and software for capturing and encrypting fingerprint data; b) A UPI service provider server for facilitating secure transmission of encrypted fingerprint data; c) An Aadhaar Authentication Server for storing and matching biometric data; d) An encryption layer implementing a hybrid encryption scheme for secure data transmission.
6. The system of claim 5, further comprising a liveness detection module to prevent spoofing attempts during fingerprint capture.
7. The system of claim 5, wherein the Aadhaar Authentication Server implements a highly parallel, multi-point comparison algorithm for fingerprint matching.
8. A non-transitory computer-readable medium storing instructions that, when executed by a processor, perform the method of claim 1.