**FORM 2**

THE PATENTS ACT, 1970

(39 of 1970)

&

THE PATENTS RULES, 2003

**COMPLETE SPECIFICATION**

(See Section 10; rule 13)

TITLE OF THE INVENTION

**PIN AUTHENTICATION SYSTEM WITH FINGERPRINTS FOR EACH DIGIT**

APPLICANT

**K.RAMAKRISHNAN COLLEGE OF ENGINEERING**

**NH-45, Samayapuram,**

**Trichy, Tamil Nadu, India– 621112**

The following specification particularly describes the invention and the manner in which it is to be performed.

# PIN AUTHENTICATION SYSTEM WITH FINGERPRINTS FOR EACH DIGIT

## TECHNICAL FIELD

The present invention is related to the field of secure authentication systems. More specifically, the current invention presents a secure authentication system which combines PIN-based authentication with biometric fingerprint recognition for each digit.

## BACKGROUND

Existing security PIN systems involve entering PINs, usually 4-6 digits, which after verification allows the user to login, and get access to a website or any application. This system is susceptible to brute force attacks, social engineering attacks and data breaches. In particular, social engineering is the way that most attackers use to get the details, directly from the authorized users by manipulating individuals to disclose the sensitive information directly. This might be a challenging subject to get rid of, as we cannot take control over the users.

Looking at the fingerprint authentication systems, there exists methodologies, through which someone can fraud the system, and get access to a website, application, or any other systems. One such way is molded fingerprints. This includes creating a fake fingerprint using molds made from materials like silicone and adhesive materials.

Such methodologies and attacks pose a threat to security, and can result in unauthorized access, scams, and misuse of data. Some organizations may offer PIN systems with long PINs, so that it would not be easier for attackers to find a number of combinations and come up with the PIN, but it also affects users' convenience in remembering longer PINs. So, they would go for easily guessable PINs, or they would simply write them down. Easy PINs like "12345678", "87654321" are prone to brute force attacks, as they fall under the most widely used passwords, across the web. Such passwords are available on the web as documents, which attackers might use to brute

force.

In highly sensitive environments like banking applications, the security risks associated with traditional PIN and fingerprint systems are particularly concerning. Thus, there is a need for a security system that is immune to such attacks. This invention, the PIN Authentication System with Fingerprint for Each Digit, addresses these issues by combining PIN authentication with individual fingerprint verification for each digit, creating a multi-layered security solution. This approach not only strengthens the security of the authentication system, but also minimizes the risk of cyber-attacks thereby making it suitable for high security applications such as banking.

## OBJECTIVE OF THE INVENTION

The primary objective of this innovation is to add a layer of security in PIN-based authentication systems by integrating fingerprint recognition for each individual digit in the PIN. The traditional PIN entry is strengthened by leveraging biometric data, which creates a multi-layer verification system to prevent unauthorized access.

Another objective of this invention is to address the vulnerabilities of traditional PIN systems, where a PIN when compromised, can be exploited easily. This system is designed in such a way that it associates each digit of the PIN with a specific fingerprint, which makes it immune to such vulnerabilities.

Yet another objective of this invention is to improve Multi-Factor Authentication (MFA), by combining PIN and biometrics into a single, simultaneous process. High-security systems which rely solely on PIN or a single fingerprint may face serious consequences when there is a data breach. Hence, this system is the advanced form of MFA.

Yet another objective of this invention is to secure data during storage and verification. Using an efficient encryption algorithm is important to achieve this. This ensures that even if the system is compromised, the data remains secure, and can be resilient against any cyber attacks.

Yet another objective of this invention is to handle multiple fingerprint sensors using a single Arduino microcontroller, since it has limited input / output (I /O) pins. Hence, it is necessary to include a multiplexer with the microcontroller unit. Multiplexer can expand the I/O capacity of the microcontroller, which enables it to handle multiple fingerprint sensors.

Yet another objective of the invention is to utilize a NoSQL database, which is suitable for managing unstructured data, in this case, the encrypted fingerprint templates. These database models are efficient for storing, retrieving and managing the data throughout the process.

Yet another objective of this invention is that, while storing the data in the database, it is important to ensure that each fingerprint template is labeled with the corresponding digit of the PIN, to prevent false positives or false negatives.

These and other objects and advantages of the present invention will become readily apparent from the following detailed description taken in conjunction with the accompanying drawings.

**SUMMARY**

The PIN authentication system with fingerprint for each digit combines PIN authentication with a biometric finger recognition system. This system is designed in such a way that adds to security by ensuring that each digit of the PIN is verified with a unique fingerprint.

The system consists of a number pad with each digit embedded with 10 fingerprint sensors. Users can enter their PIN by placing fingers corresponding to each digit in the PIN of their choice.

An input module is included to handle the credentials entered by the users. It then directs them to subsequent processes. An Arduino microcontroller connected to a multiplexer is deployed, which allows for handling multiple fingerprint sensors.

The collected data is then forwarded for the encryption process in order to secure user credentials during storage and verification. AES-256 encryption algorithm can be used for encrypting each fingerprint template along with its associated digit.The encrypted data is then stored in a NoSQL database.

A verification module is included, which retrieves the encrypted fingerprint templates and PIN from the database, decrypts them, and compares them with the user's input. It ensures accurate matching between the stored and entered credentials. An authentication module then interprets the comparison results and authenticates the user.

A digital display is incorporated to prompt the user throughout the authentication

process and display the authentication results.

The hardware components of the system include the fingerprint sensors, a microcontroller with multiplexer, a number pad, a digital display , all placed in a plastic case. The entire system is designed to offer a unique, yet secure authentication solution, hence making it suitable for banking applications.

## BRIEF DESCRIPTION OF THE DRAWINGS

The following is the detailed description and accompanying drawings of the preferred embodiment of the PIN authentication system with fingerprint for each digit in which:

Fig 1 illustrates the front view of the PIN authentication system with a fingerprint for each digit, according to the embodiment of the present invention, which includes the placement of all the hardware components utilized by the system.

Fig 2 illustrates the first isometric view of the PIN authentication system with fingerprint for each digit, according to the embodiment of the present invention, which presents the three dimensional perspective of the system.

Fig 3 illustrates the second isometric view of the PIN authentication system with fingerprint for each digit, according to the embodiment of the present invention, presenting an alternative three dimensional perspective of the system.

Fig 4 illustrates the drafting view of the PIN authentication system with fingerprint for each digit, according to the embodiment of the present invention, included for clearer understanding of the placement of components.

Fig 5 illustrates the final rendered image of the PIN authentication system with fingerprint for each digit, according to the embodiment of the present invention, which provides a visual approximation of the final product .

Fig 6 illustrates the flow of the enrolment process of the PIN authentication system with fingerprint for each digit, according to the working of the present invention, which depicts the steps the user has to go through during registration.

Fig 7 illustrates the flow of the verification process of the PIN authentication system with fingerprint for each digit, according to the working of the present invention, which outlines the steps involved in the verification process .

The material, sensors and other components used in this design may be replaced or modified in accordance with the requirements of the present invention.

Below is the list of numerals used for reference in detailed description and drawings:

1 - Digital Display, 2 - Number Pad, 3 - Plastic Case & 4 - Sensors embedded with the number keys.

## DETAILED DESCRIPTION

The following detailed description illustrates the various embodiments and the other advancements and features that are illustrated in the detailed description. The examples used herein are intended to facilitate the understanding of ways in which the embodiments herein operate.

The PIN authentication system with fingerprint for each digit is designed to integrate biometrics with PIN-based authentication. The basic aim is to implement a secure system that is immune to commonly known attacks. This system provides security by requiring not only the correct PIN, but also a fingerprint scan for each individual digit entered. This type of solution is particularly used for sensitive applications such as banking, where unauthorized access could lead to serious consequences.

The PIN authentication system with fingerprint for each digit utilizes at least 10 sensors, each associated with a digit of the PIN. These sensors are embedded in a number pad, allowing each digit entry to correspond with a specific fingerprint scan. An Arduino microcontroller, connected to a multiplexer is included to handle multiple fingerprint sensors. As the Arduino has limited I/O pins, the multiplexer is used in place to expand the microcontroller's capacity. In this context, the multiplexer is used to selectively activate each fingerprint sensor as per the sequence. Multiplexers simplify the wiring within the sensors which allows to create less complex systems. Another reason for using multiplexers in this system is that they reduce interference. This means that fingerprint images and data collected are cleaner and clearer.

During the enrollment process, the input module guides the user to scan a fingerprint for each digit of the PIN as they enter it. When the user enrolls, the input module prompts the user to simultaneously scan a fingerprint for each digit they enter. For example, if the PIN the user chooses is "1234", he/ she may enter '1' with the index

finger, ‘2’ with the thumb finger, ‘3’ with the ring finger, and ‘4’ with the middle finger. This provides an additional layer of security, since, even if someone knows the PIN, they cannot authenticate without entering the correct sequence of fingerprints for each digit.

Once the fingerprints are captured , the captured fingerprint templates are then encrypted using the AES-256 encryption algorithm, a widely used robust symmetric key encryption method. Since it is a symmetric key algorithm, it means that the same key is used for both encryption and decryption. The encrypted fingerprint data is stored in a NoSQL database such as MongoDB or Firebase, labeled with the digit of the PIN which it corresponds to. For example, the fingerprint captured for ‘1’ is labeled as associated with digit 1. The main reason for using these databases is that they offer high flexibility and scalability.

Once the enrollment is done, the system can be used for authentication. To authenticate, the user must enter the PIN as usual, i.e the user must place the corresponding finger for each digit of the PIN. This part is handled by the input module.

The verification module retrieves the encrypted fingerprint template stored in the database. It then decrypts the data using the AES encryption key, and compares it with the freshly captured fingerprints . If the decrypted fingerprint matches the captured fingerprint, and the PIN is correct, the authentication module confirms the user’s identity and grants access. This precise matching process ensures that only authorized users can pass through the authentication successfully.

By encrypting both the fingerprint templates and as well as the PINs associated with it , this system prevents unauthorized access and tampering of sensitive data. The use of the AES-256 encryption algorithm provides an extra layer of protection, ensuring that even if someone intercepts the data, they will not be able to decrypt it without the correct key.

The NoSQL database plays a crucial role in storing and handling the large volume of biometric fingerprint templates associated with various PIN digits. This database solution also supports high scalability and performance, which helps in retrieval of data when needed. Due to these features, it is suitable for use in high-security environments where numerous users may need to enroll and authenticate.

In summary, this system offers an innovative solution by combining PIN authentication with biometric fingerprint recognition for each digit.The use of AES-256 encryption ensures that all the fingerprint data remains secure, and the NoSQL database offers wide and efficient storage and also retrieval of biometric data. With its high level of security and ease of use, this system can be implemented in various high- security applications, especially in banking applications,where safeguarding sensitive data is crucial.

Albert Francis
Application Agent(INPA - 4655)

## CLAIMS

**We claim that,**

1. A PIN authentication system with fingerprint for each digit, comprising:

a number pad, which integrates at least 10 fingerprint sensors where each sensor corresponds to one digit (0-9) of the PIN, for the user to enter their credentials through both PIN input and fingerprint recognition;

an input module, to handle the user-entered credentials and direct the data for encryption process;

a microcontroller unit, for handling multiple fingerprint sensors by selectively activating each sensor as per the input sequence;

an encryption module, for encrypting both the PIN and the corresponding fingerprint templates for each digit of the PIN, ensuring data security during storage and retrieval;

a database, for storing the encrypted fingerprint templates labeled with their corresponding digits of the PIN for identification during verification;

a verification module, to retrieve, decrypt, and compare the user-entered credentials, including the PIN and associated fingerprint data, for authentication purposes;

an authentication module, which interprets the comparison results from the verification module and authenticates the user based on a match; and

a digital display, which guides the user throughout the authentication process by providing prompts and displays the final authentication result.

2. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein the hardware components, including the number pad and capacitive fingerprint sensors assigned to each digit of the PIN, are connected to the microcontroller unit, which handles fingerprint recognition associated with each digit.

3. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein the input module prompts the user to enter credentials via a digital display and directs the collected data for the encryption process.

4. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein an Arduino microcontroller connected to a multiplexer is employed to manage multiple fingerprint sensors, which can handle data collection from each sensor.

5. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein the encryption module utilizes the Advanced Encryption Standard algorithm to encrypt the user-entered PIN and associated fingerprint templates, to protect the data during storage and verification.

6. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein the database utilizes a NoSQL storage model to store the encrypted fingerprint templates and associated PIN data for efficient retrieval during verification processes.

7. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein the verification module retrieves the stored data, decrypts it, and compares it with the user-entered credentials, searching for a match to authenticate the user.

8. The PIN authentication system with fingerprint for each digit, as claimed in claim 1, wherein the authentication module interprets comparison results from the verification module and authenticates the user based on successful matching of both the PIN and associated fingerprint data.

9. The PIN authentication system with fingerprint for each digit, as claimed in claim 2, wherein alternative types of fingerprint sensors, such as optical sensors and ultrasonic sensors, can also be integrated to perform fingerprint recognition for each digit.

Albert Francis
Application Agent(INPA - 4655)

## ABSTRACT

### PIN AUTHENTICATION SYSTEM WITH FINGERPRINT FOR EACH DIGIT

The present innovation discloses a PIN authentication system with fingerprint for each digit to provide an added layer of security to the existing PIN-based authentication systems. The system incorporates a number pad embedded with fingerprint sensors on each digit to allow users to enter a PIN with corresponding fingers. An input module directs the user-entered credentials to an Arduino microcontroller connected to a multiplexer, which manages multiple fingerprint sensors. Advanced Encryption Standard algorithm is made use by the system to secure the fingerprint templates and associated PIN digits, which are then stored in a NoSQL database for data management. The verification module retrieves and decrypts the stored data and compares them with the user-entered data. The comparison results are interpreted by the authentication module to authenticate the user. A digital display guides the users throughout the process and displays authentication results. This system is suitable for high-security systems like banking, where security is of major concern.