Fingerprint Recognition for Future ATM Security

M. N. Narsaiah, Gangalam Lasya, Kondamudi Veronica, Abhilash, Padaga Sravya Kirthana, M. Santoshi Kumari and Ashish Pathani

1,2,3,4,5 Department of Electronics and Communication Engineering, KG Reddy College of Engineering & Technology, Telangana, India
6 Assistant Professor, Department of CSE(AIML), GRIET, Bachupally, Hyderabad, Telangana
7 Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, 248007

Abstract. Today, it is typical to need to identify and validate a person in order to use a safe box, operate a vehicle, access a bank account via an ATM, or carry out other operations that call for the protection of personal information. The accuracy and dependability of traditional methods, such as ID card verification or signature, are lacking. The systems in use at these places must be rapid and dependable. The usage of ATMs, which allow users to conveniently exchange banknotes, is now met with a new challenge: guaranteeing that users can maintain a valid identification. Customers are experiencing financial losses as a result of the increase in criminal cases brought about by antiquated ATM identification procedures. Our system's main objective is to improve the usability and security of online transactions. Today, the application of biometric technologies is expanding swiftly. Biometrics is used for personal identification. Here, we are allowing user’s access to an ATM by means of a biometric fingerprint scanner. The Bank enters a fingerprint's information into a database during the enrolment procedure. The bank provides authentication to the customer, which they can use to conduct transactions. If a fingerprint match in the database occurs, transactions take place. The transaction will be cancelled if, following verification, the fingerprint does not match. The user of a fingerprint-based ATM machine can conduct secure transactions.

Keywords: ATM, Accessing, Authentication, Embedded System, Biometrics, Verification, Fingerprint, Security.

1 Introduction

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).
One kind of automated teller machine (ATM) recognizes individuals using fingerprint technology. Instead of requiring a PIN or card to access an account, a fingerprint-based ATM machine verifies a person's identity using their unique fingerprint. The technology behind fingerprint-based ATMs is based on biometric identification, which involves verifying a person's identity using bodily traits like their fingerprint, iris, or face. A user would place their finger on a sensor in an ATM equipped with fingerprint recognition technology, which would scan it and compare it to a database of fingerprints already on file. If the user's fingerprint matched one that had been previously saved, access to their account would be granted. Using fingerprint-based ATMs may have a lot of benefits, including increased convenience and security. Because fingerprints are unique to each individual, using them to verify identity can be more secure than using a PIN or a card, which can be lost or stolen. Additionally, utilizing an ATM with a fingerprint reader frees users from carrying cards or remembering PINs, which can be especially helpful for elderly or visually challenged customers. In conclusion, the use of fingerprints in ATMs represents a new and perhaps practical application of biometric technology in the financial sector. Additional research and development will be necessary to address potential issues and ensure that these gadgets can be used effectively and safely by a variety of users.

2 Literature Study

Bhagwan S. Chandrasekhar: For example, security is a top priority in today's environment in all facets of life. A variety of communication connection attacks seriously impede information transfer. To protect data against hackers, many security algorithms are available. The biometric authentication procedure gives an additional layer of security for anyone who is sensitive to authentication. This study provides a highly secure and energy-efficient ATM banking system as an alternative to the current system [1].

Benson M. Onywoki: ATM use has become crucial in the financial industry as a result of the value that may be transacted utilizing these systems and their frequent use. Despite the fact that many academics have looked at the use of biometrics in security applications for financial institutions, no systematic empirical research has been done to examine the role of organizational characteristics and contextual factors in the Kenyan financial sector. This study used the framework it had built to variables affecting the adoption of biometric ATMs in the Kenyan banking industry in order to study factors influencing the adoption of biometric ATM authentication [2].

Sangeetha Thirumoorthy: In the modern world, everyone uses ATMs, which allow for cash transfers and withdrawals. The basis of this work is the fingerprint technique utilized in the ATM System. We chose this area to improve people's security and safety while facilitating...
transactions. The fingerprints on each individual are unique. You don't have to keep an
ATM card on you at all times, and there is no chance of losing one. Fingerprint technology
outperforms other ATM security solutions in terms of dependability and safety. These
aspects both provide a consistent environment between customers and ATMs and make this
method a straightforward and secure way of transaction [3]

Kruti Harkhani: In the present era, the ATM system is a crucial component of our daily life.
In order to conveniently handle their banking demands, people have relied significantly on
and trusted automatic teller machines, or ATMs, for the past three decades. Traditional
ATM systems authenticate primarily using the debit card and password; nevertheless, this
method has significant limitations. The debit card and password cannot be used to confirm
the precise user's identity. The password and user's debit card are illegally taken when
thieves tamper with the ATM terminal [4]

Shaikh Mohd Faiz: Today, security is a top priority in many facets of life. Numerous
attacks on the communication link substantially impede information delivery. There are
numerous security algorithms available to protect data from hacking. The use of biometrics
gives an additional degree of security for anyone who is sensitive to authentication. The
ATM banking system described in this paper is far more secure and environmentally
friendly than the current system. The majority of ATM systems use the triple data
encryption standard at the moment [5]

Usha Rani R: Our concept proposes employing OTP and fingerprint authentication as the
password in ATMs in place of the traditional pin number. Because fingerprint recognition
enables users to keep their accounts private and prevents unauthorized access, users will
feel more at comfortable using it. Our system has both fingerprint authentication and an
OTP capability. It will be impossible for any criminal to use the password to carry out any
sort of fraud because the OTP can only be used once. As a result, even if a criminal gets
hold of it, it can no longer be used in the future [6]

3 Existing System

The current ATM system uses a card and PIN-based method to authenticate transactions.
Following that, it gives bank clients access to a number of services like cash withdrawals
and deposits, account-to-account transfers, balance inquiries, top-up purchases, and utility
bill payment. The ATM system verifies each user's entered PIN against the permission PIN
that has been previously stored. If a match is found, the system authenticates the user and
provides them access to all of the ATM's functions. On the other hand, if there is a
mismatch, the user authentication procedure fails, and the user is given two additional
chances to enter a proper PIN. The card is blocked and kept by the ATM if an erroneous
PIN is entered three times

4 Proposed System

In our nation, we conduct all of our banking business through ATMs. With the help of an
automated teller machine (ATM), customers of financial institutions can conduct financial
transactions like cash withdrawals, deposits, fund transfers, and account information at any
time and without having to speak with bank employees directly. The door opens and the
user's name is displayed on the LCD monitor when a user scans their finger in our
suggested system, and the door closes within 10 seconds of transaction activity if the user is
legitimate. In our nation, we conduct all of our banking business through ATMs. With the help of an Automated Teller Machine (ATM), customers of financial institutions can conduct financial transactions like cash withdrawals, deposits, fund transfers, and account information at any time and without having to speak with bank employees directly. The door opens and the user's name is displayed on the LCD monitor when a user scans their finger in our suggested system, and the door closes within 10 seconds of transaction activity if the user is legitimate.

5 Methodology

- Arduino Uno
- Finger Print Sensor
- Keypad
- DC Motor
- LCD
- Regulated Power Supply

5.1 Description of Hardware Components

5.1.1 Arduino UNO

An open-source microcontroller board called Arduino Uno is based on the ATmega328P microcontroller. It has a 16 MHz quartz crystal, 6 analogue inputs, 14 digital input/output
pins (of which 6 can be used as PWM outputs), a USB port, a power jack, an ICSP header, and a reset button. It offers a user-friendly platform for hobbyists, artists, and developers to construct interactive projects and is frequently utilized in a variety of electronic projects. The Wiring-based Arduino programming language and the Arduino Integrated Development Environment (IDE) are used to create programs for the Arduino Uno.

5.1.2 Fingerprint Sensor

For identification and authentication applications, a fingerprint sensor is a type of biometric sensor that is used to record and examine a person's distinctive fingerprint features. The sensor is often an electronic gadget that scans and records the ridges, whorls, and other distinguishing characteristics on a person's fingertip, producing a digital image of their own biometric template. The identity of the person seeking to access a certain system, device, or service is then verified by comparing this template to a database of previously captured fingerprints.

5.1.3 Keypad

Typically used to enter numeric or alphabetic characters into electronic devices or systems, a keypad is a series of buttons or keys arranged in a grid or matrix arrangement. Numerous gadgets, such as telephones, calculators, cash registers, security systems, and Automated Teller Machines (ATMs), have keypads.

5.2 Description of Software Components

5.2.1 Arduino IDE

Programming and writing code for Arduino microcontroller boards is done using the software program known as the Arduino IDE (Integrated Development Environment). For creating, building, and uploading code to Arduino boards, the IDE offers a user-friendly interface.

The Arduino IDE has a library of pre-written code and utilities that can be used to streamline development and supports a number of programming languages, including C and C++.

A serial monitor is another feature of the IDE that enables developers to interact with the microcontroller board and view its output in real time. The Arduino IDE is free to download from the Arduino website and is open-source software.

Numerous operating systems, including Windows, Mac OS X, and Linux, are compatible with it. In a multitude of domains, including robotics, electronics, and automation, the IDE is widely utilized by professionals, students, and amateurs.

5.2.2 Embedded C

A programming language called embedded C is used to create software for embedded systems, which are computers created to carry out certain functions within larger systems. An adaptation of the C programming language called embedded C is designed for usage in contexts with limited resources, including microcontrollers and other embedded systems. A selection of specialized data types and functions created specifically for embedded devices
are offered by embedded C. It is intended to operate in tandem with the system's hardware, giving low-level access to device registers and other hardware parts.

Applications for embedded C include consumer electronics, industrial control systems, medical equipment, and automotive systems. It is a strong and adaptable programming language that enables programmers to create dependable and effective code for a variety of embedded devices.

Typically used to enter numeric or alphabetic characters into electronic devices or systems, a keypad is a series of buttons or keys arranged in a grid or matrix arrangement. Numerous gadgets, such as telephones, calculators, cash registers, security systems, and Automated Teller Machines (ATMs), have keypads. Place the figure as close as possible after the point where it is first referenced in the text. If there is a large number of figures and tables, it might be necessary to place some before their text citation.

Numerous operating systems, including Windows, Mac OS X, and Linux, are compatible with it. In a multitude of domains, including robotics, electronics, and automation, the IDE is widely utilized by professionals, students, and amateurs.

5.2.3 **Operation**

1. The suggested method does not require a card or PIN to function, which makes it an upgrade over the current system.

2. The suggested system exclusively uses biometric fingerprints; customers use their fingerprints at ATMs, and if they match properly, the system operates.

3. The customer then chooses the back to transaction with option, followed by the account type for the bank they have an account with.

4. Next, decide whether to withdraw money, check your account balance, and so forth. The consumer will now select or decide.

5. The bank from which he wishes to withdraw funds, specifying whether it is a current or savings account,

6. This is a technique for employing biometric fingerprints to secure ATM transactions. There are many benefits to the suggested approach over the existing Card and PIN method

6 **Results**

1. The outcome is evaluated by comparing the ATM system's security components or by matching the PIN-Code.
2. The system's final outcome is determined by matching fingerprint patterns.
3. In addition to the standard methods of accurately entering client fingerprints that were sent by the administrator and verified, the execution of ATM protection by fingerprint also includes those techniques.
4. The protection function was greatly enhanced to ensure that the client's identity was firm and stable.
5. The entire system was built using a fingerprint technology, making it secure, dependable, and simple to use.
6. This will be the most advantageous technology for digital or electronic money transactions.

![Verification of fingerprint](image1)

**Fig. 2.** Verification of fingerprint

![Display of result for fingerprint](image2)

**Fig. 3.** Display of result for fingerprint.

### 7 Conclusion

As we are all aware, robberies have recently targeted the majority of ATMs. Additionally, ATM theft has been steadily rising year after year. The automation of "ATM THEFT" prevention from robbery is demonstrated in this article. Autonomous systems are crucial to our daily lives in the contemporary world. The rapid development in societal computerization and automation is clearly visible in the areas with an increasing number of ATM locations. Most civilians frequently use ATMs. A financial transaction, the simplicity of money exchange, etc., are good examples. Security is a significant factor, therefore. The amount of crime involving financial institutions has dramatically increased. 90% of incidents in ATM centers over the past few years have taken the form of robberies. Both bank management and the general public are seriously threatened by this problem. Therefore, using...
This study suggests a way to reduce ATM robberies in real-time. The design's primary goal is to deter ATM theft. The main driving force behind this endeavor has been a number of current events. It is already commonplace and trustworthy to employ fingerprint technology for secure authentication and identification. The way we protect our assets, technology, and private information has undergone a transformation. Due to the growing popularity of fingerprint technology, it is increasingly essential to understand both its benefits and limitations. One of the key advantages of fingerprint technology is convenience. It eliminates the need to carry several access cards or keep track of intricate passwords. Additionally, it ensures that only those with authorization can access private information or locations. Fingerprint technology is also particularly secure because it is based on a specific biometric characteristic that is challenging to imitate or forge. Numerous industries have used fingerprint technology to a significant degree, including finance, healthcare, and law enforcement. It is extensively used in consumer gadgets as well, including computers, tablets, and smartphones. The widespread use of fingerprint technology has reduced the danger of fraud and identity theft while increasing security. There are significant limitations to the fingerprint technology, though. The major disadvantage is that, depending on the circumstance, fingerprints can be stolen or hacked.

References