Cardless and Secure ATM Cash Withdrawal for Rural Areas

Sarala B[1],Rakshana S[2],Sahana B[3],Sakthi Maheswari M[4]

[1]Assistant Professor, Electronics and Communication Engineering,

Sri Venkateswara College of Engineering-602117

[2,3,4] UG student, Electronics and Communication Engineering,

Sri Venkateswara College of Engineering-602117

Corresponding author:sarala@svce.ac.in

2020ec0712@svce.ac.in

2020ec0070@svce.ac.in

2020ec0697@svce.ac.in

Abstract

An imminent revolution in ATM transactions is poised to tackle the shortcomings of traditional card-based systems. Relying on physical cards exposes users to theft and misplacement risks, exacerbated by the management of multiple cards. Introducing the innovative solution: a cardless ATM transaction process. This groundbreaking method allows users to effortlessly authenticate themselves using their unique fingerprints, eliminating the need for easily lost physical cards. Authentication involves meticulously comparing fingerprints with registered data, ensuring stringent security measures. Upon successful verification, users gain access to their bank accounts, each requiring a specific PIN. Advanced encryption techniques, such as AES, significantly bolster the security of this process. Connection between the user's verification device and the ATM is seamlessly established using Zigbee technology, bypassing the necessity for an internet connection. Once the correct PIN is input, users can seamlessly conduct transactions, including withdrawals and deposits. Noteworthy is the system's capability to designate guest users and grant transaction authorization, ensuring secure transaction approval even in the absence of the primary user, thereby enhancing peace of mind. The implementation of this groundbreaking project holds the promise of revolutionizing ATM transactions, enhancing both security and convenience. Furthermore, its independence from internet connectivity renders it suitable for regions with poor connectivity or challenging environmental conditions, underscoring its accessibility and adaptability. In essence, this innovative system heralds a new era for ATM transactions, delivering heightened security and convenience, poised to redefine financial transactions.

Keywords: Cardless, ATM, biometry, authentication, AES encryption, SHA-256, Zigbee.

1. Introduction

The rise of digital technology has transformed banking and finance, leading to innovations in secure transaction methods. This paper presents a novel solution for cardless ATM withdrawals using biometric authentication, leveraging a fingerprint sensor for seamless identification. Two modes are explored: fingerprint-based authentication and a "friend option" with a temporary PIN, addressing security challenges through cryptographic techniques. This approach enhances user convenience and ensures robust security.

2. System Architecture

2.1 Fingerprint Sensor

Users engage with the ATM application via a fingerprint sensor, whereupon placing their finger on the sensor which is depicted in fig 1, the system captures and verifies the fingerprint against pre-existing templates for authentication. This secure process ensures user identity before proceeding with transactions.

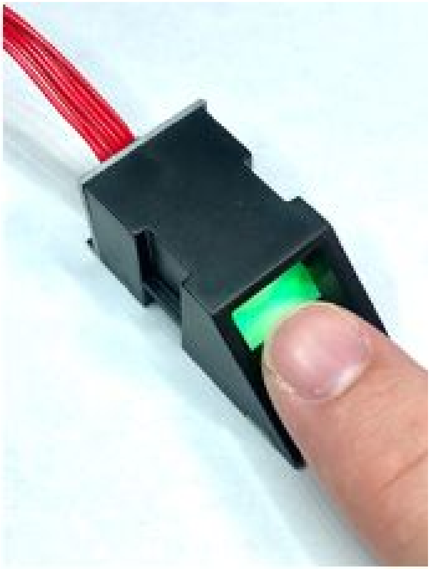
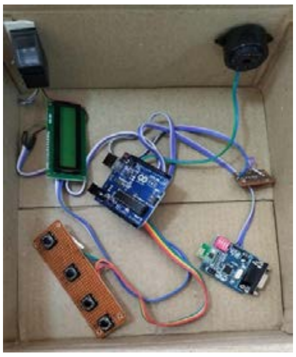


Figure 1. Fingerprint sensor

2.2 Zigbee Transmitter and Receiver



The hardware components of the system communicate with the software application via Zigbee technology. Specifically, the Zigbee transmitter, linked to the microcontroller, sends the fingerprint ID to the receiver, which is then connected to the device hosting the software application, facilitating seamless integration and data transfer between the physical and digital components.

2.3 Buzzer and LED

The buzzer and LED serve as indicators to notify the user of successful authentication. A green LED illuminates upon a fingerprint match, while a red LED lights up and the buzzer sounds if the fingerprint does not match. This system provides clear feedback for user authentication status.

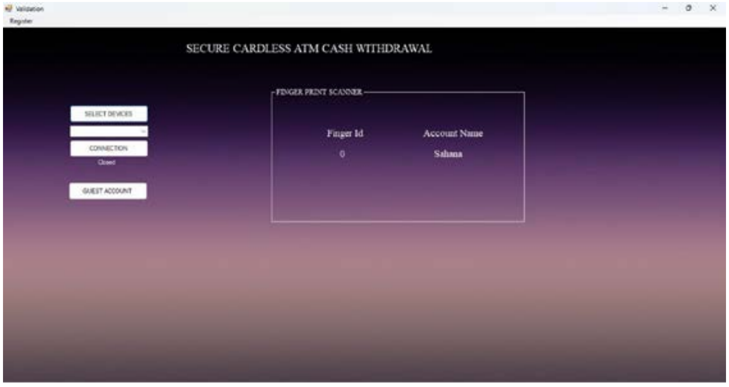
2.4 LCD and Push Buttons

The LCD screen provides guidance to users on operating the hardware, offering instructions for utilizing the fingerprint sensor. Additionally, the push buttons enable users to enroll, verify, or delete their fingerprints directly on the hardware interface. This user-friendly system ensures efficient management of fingerprint data.

Figure 2. Hardware setup

2.5 User Interface

The ATM application offers a user-friendly platform for managing transactions, allowing users to opt for their desired bank, select between deposit and withdrawal functions, and input transaction specifics.



Finger Id	Account Name
0	Sahana

Figure 3. User Interface

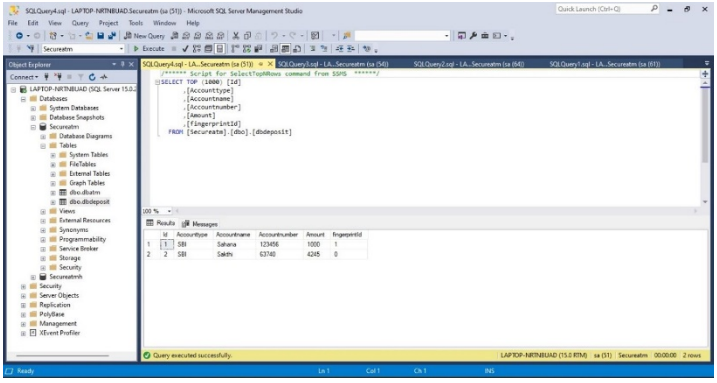
2.6 Microsoft SQL Database

The Microsoft SQL Server Management Studio emulates the functionality of the ATM server, housing tables that securely store and present user credentials and transaction information. Equipped with integrated encryption and auditing features, this tool guarantees the integrity of data and adherence to regulatory standards.

Figure 4. SQL Database

2.7 Types of Authentication

2.7.1 Fingerprint-Based Authentication: After successful fingerprint verification, users are directed to the transaction page. The system securely stores only a template of the fingerprint, not the original image, ensuring security. Users then enter their PIN, which is transmitted securely to the server.



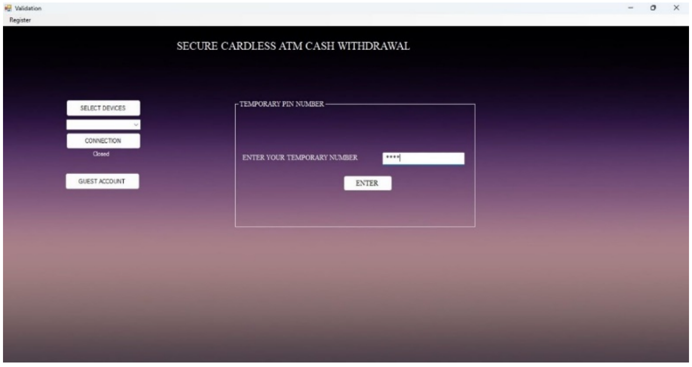
```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [Id]
      ,[Accounttype]
      ,[Accountname]
      ,[Accountnumber]
      ,[Amount]
      ,[fingerprintId]
  FROM [Secureatm].[dbo].[dbdeposit]
```

	Id	Accounttype	Accountname	Accountnumber	Amount	fingerprintId
1	1	SBI	Sahana	123456	1000	1
2	2	SBI	Sakthi	63740	4245	0

Query executed successfully. LAPTOP-NRTNBUAD (15.0 RTM) sa (51) Secureatm 00:00:00 2 rows

2.7.2 Friend option: Users can select a "friend" option, wherein they establish a temporary PIN. This PIN remains effective for a specified duration, such as 4 hours, during which users can access the application using the temporary PIN instead of their fingerprint.

Figure 5. User Interface (Friend Account)



ENTER YOUR TEMPORARY NUMBER ****

2.8 Security Measures

To ensure PIN security, a two-step process is followed

2.8.1 Hashing: The user's PIN undergoes hashing via the SHA-256 algorithm, a member of the SHA-2 family renowned for safeguarding digital data. This algorithm produces a consistent 256-bit hash value, guaranteeing the integrity and authenticity of the data. Originating from the NSA, SHA-256 employs cryptographic techniques on input data to generate a distinct and exceptionally secure hash value. Its extensive usage in blockchain technology, digital signatures, and password hashing underscores its trustworthiness in preserving data security.

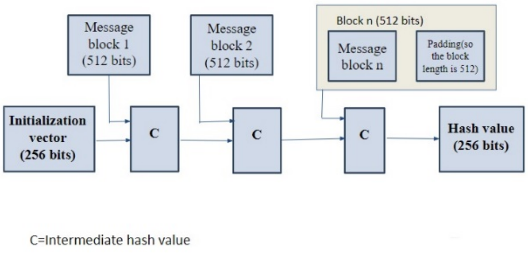

Message block 1 (512 bits)
Message block 2 (512 bits)
Block n (512 bits)
Message block n
Padding(so the block length is 512)
Initialization vector (256 bits)
C
C
C
Hash value (256 bits)
C=Intermediate hash value

Figure 6. SHA-256 Algorithm

2.8.2 AES Encryption: Before transmission, the hashed PIN undergoes encryption using the AES algorithm. AES, short for Advanced Encryption Standard, stands as a widely adopted encryption method, guaranteeing the security of data transmission and storage. Developed by NIST, it employs symmetric key cryptography and functions on fixed-size data blocks. With key lengths of 128, 192, or 256 bits, AES encryption boasts formidable resistance against attacks owing to its numerous rounds of operations. Its efficacy, adaptability, and robust security attributes render it indispensable for safeguarding communication channels, data at rest, and information traversing networks.

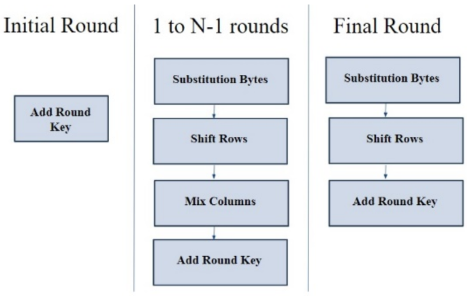


Figure 7. AES Algorithm (Rounds Details)

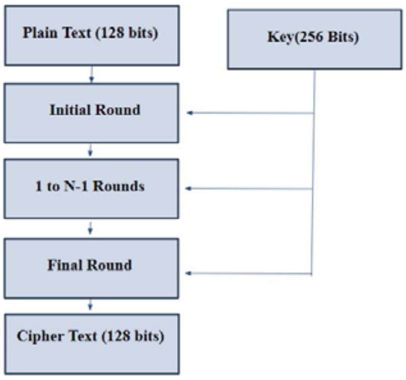


Figure 8. AES Algorithm (Overall Block)

3. Implementation Details

The ATM application was developed using Visual Studio, utilizing the C# programming language known for its object-oriented nature and robust library support. This language is well-suited for crafting scalable, secure, and high-performance applications. Integration with hardware components was achieved through Arduino microcontroller, with code written in Embedded C using the Arduino IDE platform. Cryptographic libraries were employed for secure handling of PINs. Communication between the ATM and user devices was facilitated by Zigbee modules, operating on the IEEE 802.15.4 standard, ensuring reliable connectivity. Zigbee's mesh networking capabilities promote self-healing networks, enhancing reliability, while its low power consumption extends device longevity. With its small packet size and minimal latency, Zigbee efficiently caters to applications such as home automation and sensor networks. Its interoperability and support for secure protocols render it versatile for various use cases.

4. Applications

- Introducing an alternative withdrawal method for bank account holders, aiming to provide greater flexibility and convenience.
- Implementing multi-layered authentication protocols to bolster security measures.
- Enabling users to seamlessly switch between linked accounts securely via biometric authentication.
- Embracing a trend towards reduced dependence on traditional cards for future transactions.
- Exploring integration opportunities for technological advancements in transaction processes.
- Enhancing accessibility features to cater to individuals with disabilities.
- Integrating with smart home systems to deliver tailored transaction experiences.

5. Conclusion and Future Scope

The cardless and secure ATM cash withdrawal system presents a robust alternative to traditional card-based transactions. By utilizing biometric authentication and secure communication channels, we improve user convenience while upholding strict security standards. This solution eliminates the necessity for an internet connection, making it well-suited for implementation in rural areas where internet access may be limited. Our future endeavors include scalability testing, conducting usability studies on ZigBee as a mobile portable device, and real-world deployment. Additionally, it resolves the challenges associated with managing multiple cards for multiple accounts, offering a more streamlined management option. This solution has the potential to significantly reduce card-related fraud and deliver a seamless transaction experience for users.

6. References

[1] Kaushik, Bharti & Malik, Vikas & Saroha, Vinod. (2023). A Review Paper on Data Encryption and Decryption. International Journal for Research in Applied Science and Engineering Technology. 1986-1992. 10.22214/ijraset.2023.50101.

[2] Pronika, Pronika & Tyagi, S.. (2021). Performance analysis of encryption and decryption algorithm. Indonesian Journal of Electrical Engineering and Computer Science. 23. 1030. 10.11591/ijeecs.v23.i2.pp1030-1038.

[3] Oruh, Jane. (2014). Three-Factor Authentication for Automated Teller Machine System. International Journal of Computer Science and Information Technology. 4. 160-166.doi: 10.1109/ICCT46805.2019.8947111.

[4] Samir Chabbia, Rachid Boudoura, Fouzi Semchedineb, and Djalel Chefrour, "Dynamic array PIN: A novel approach to secure NFC electronic payment between ATM and smartphone", Published online: Information Security Journal: A Global Perspective, Jun 2020, pp. 1-14.

[5] L. Chang, "The Research on Fingerprint Encryption Algorithm Based on The Error Correcting Code," 2022 International Conference on Wireless Communications, Electrical Engineering and Automation (WCEEA), Indianapolis, IN, USA, 2022, pp. 258-262, doi: 10.1109/WCEEA56458.2022.00061.

[6] B. V. Varun, A. M.V., A. C. Gangadhar and P. U., "Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1391-1395, doi: 10.1109/ICCT46805.2019.8947111.