BIOMETRIC AUTHENTICATION FOR ATM TRANSACTIONS USING FINGERPRINT RECOGNITION

[1] Ch. Srilakshmi,[2] Setty Sravani, [3] Midde Raja Sekhar,[4] K.Anjaneya Prasad
[1]Assistant Professor,[234]Research Assistant
Department Of Computer Science & Engineering
Dr.K.V. Subba Reddy Institute Of Technology, Kurnool, A.P.

ABSTRACT
ATM security has become a critical concern due to the increasing incidents of fraud, card skimming, and unauthorized access. Traditional ATM authentication methods, such as PIN-based verification and magnetic stripe cards, are vulnerable to theft and hacking. To address these security challenges, this study proposes a Biometric Authentication System for ATM Transactions Using Fingerprint Recognition. The system utilizes fingerprint biometrics as a unique and secure authentication mechanism, eliminating the need for PINs and physical cards. The proposed approach integrates high-resolution fingerprint scanners with a secure encryption framework, ensuring accurate user verification and preventing identity theft. The system is designed to operate in real-time, offering faster transaction processing, reduced fraud risks, and enhanced user convenience. Experimental results demonstrate the system's high authentication accuracy, minimal false acceptance rates, and improved security compared to conventional ATM systems. This research highlights the effectiveness of biometric-based authentication in financial transactions and paves the way for next-generation secure banking solutions.

I. INTRODUCTION

With the rise of digital banking and cashless transactions, ATM security has become a major concern due to increasing incidents of card fraud, PIN theft, and unauthorized access. Traditional authentication methods, such as magnetic stripe cards and PIN-based verification, are highly susceptible to security threats like card skimming, shoulder surfing, and hacking attacks. These vulnerabilities pose risks to both financial institutions and customers, leading to financial losses and compromised user data.

To enhance security and eliminate dependency on physical cards and passwords, biometric authentication has emerged as a more reliable, secure, and user-friendly alternative. Fingerprint recognition, in particular, provides a unique and tamper-proof method of identification, ensuring that only authorized users can access their accounts. Unlike PINs, which can be forgotten or stolen, fingerprints are unique to individuals and difficult to replicate, making them an ideal choice for secure banking transactions.

This study proposes a Biometric Authentication System for ATM Transactions Using Fingerprint Recognition, integrating advanced fingerprint scanning technology with encrypted biometric databases to enhance ATM security. The system aims to:

1. Eliminate card-related fraud by replacing ATM cards with fingerprint authentication.
2. Ensure secure and seamless transactions through encrypted biometric verification.
3. Improve user convenience by reducing dependency on PINs and preventing unauthorized access.

By leveraging biometric authentication, this system provides a highly secure, fast, and efficient solution for modern banking environments. The following sections explore the literature review, system methodology, implementation, and performance analysis of the proposed fingerprint-based ATM security system.

II. LITERATURE SURVEY

The advancement of biometric authentication in financial transactions has gained significant

attention due to its enhanced security, fraud prevention, and user convenience. Several studies have explored the application of fingerprint-based ATM systems to replace traditional card and PIN-based authentication methods. This section reviews existing research on ATM security, fingerprint recognition technology, and biometric authentication frameworks.

1. Traditional ATM Security Methods and Their Limitations

Early ATM systems relied on magnetic stripe cards and PIN authentication, which introduced several security vulnerabilities, including card skimming, phishing attacks, and PIN theft. Jain et al. (2015) highlighted the increasing incidents of ATM fraud and card duplication, emphasizing the need for more secure authentication methods. Sharma et al. (2016) analyzed PIN-based security risks and suggested that biometric authentication could offer a more robust and user-friendly solution.

2. Fingerprint Recognition in Biometric Security

Fingerprint recognition has been widely studied as an effective biometric authentication method due to its uniqueness, stability, and difficulty to forge. Maltoni et al. (2017) demonstrated that fingerprint biometrics provide a high level of accuracy and security in identity verification. Ratha et al. (2018) proposed a secure fingerprint template storage mechanism, ensuring that biometric data remains encrypted and protected against unauthorized access.

3. Implementation of Fingerprint Authentication in ATMs

Several studies have explored fingerprint-based ATM security frameworks. Kumar et al. (2019) introduced an embedded fingerprint scanner for ATM authentication, reducing dependency on physical cards and preventing identity theft. Singh and Verma (2020) developed a hybrid security system integrating fingerprint biometrics with facial recognition to further enhance ATM security. Zhang et al. (2021) implemented a cloud-based fingerprint authentication system, improving real-time transaction processing and fraud detection.

4. Comparative Analysis of Biometric ATM Security Systems

Researchers have compared different biometric authentication techniques for ATMs, including fingerprint recognition, facial recognition, iris scanning, and voice authentication. Patel et al. (2022) found that fingerprint authentication was the most cost-effective and widely accepted method due to its ease of use and high verification accuracy. However, studies also pointed out challenges such as fingerprint scanner reliability, sensor degradation, and potential spoofing attacks, which require additional security layers like liveness detection and encryption mechanisms.

Research Gap and Motivation

Despite the progress in fingerprint-based ATM security, challenges remain in ensuring real-time authentication, secure biometric data storage, and resistance against spoofing attacks. Current studies focus on improving hardware efficiency, but there is still a need for enhanced encryption techniques, multi-factor biometric authentication, and AI-driven fraud detection. This research aims to develop an optimized fingerprint-based ATM authentication system with enhanced security measures, fast processing, and encrypted biometric storage, providing a highly secure and user-friendly solution for banking transactions.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

ATM authentication has primarily relied on magnetic stripe cards and PIN-based verification, which expose users to risks such as card skimming, PIN theft, and unauthorized transactions. Fraudsters use techniques like shoulder surfing, phishing attacks, and duplicate card cloning to gain access to user accounts. Although some systems have incorporated chip-based smart cards, these methods still depend on physical possession and password security, making them vulnerable to loss, theft, or hacking. Additionally, manual entry of PINs leads to human errors, forgotten credentials, and delays

in transactions, reducing the efficiency of banking services. The lack of biometric authentication and real-time fraud detection further limits the security and reliability of these ATM systems.

Disadvantages of the Existing System:

1. Susceptibility to Fraud – Card skimming, phishing, and PIN theft increase unauthorized access risks.
2. Dependency on Physical Cards – Users must carry cards, which can be lost, stolen, or duplicated.
3. Lack of Biometric Security – No direct user verification, making authentication vulnerable to identity theft.

PROPOSED SYSTEM

To enhance ATM security and eliminate fraud risks, the proposed system implements fingerprint-based biometric authentication as a secure and efficient alternative to card-based systems. By integrating high-resolution fingerprint scanners with encrypted biometric databases, the system ensures that only the account holder can access their account, eliminating the need for physical cards and PINs. Additionally, AI-driven anti-spoofing techniques detect fake fingerprints, preventing fraud attempts. The system also incorporates cloud-based biometric storage with advanced encryption protocols, ensuring data integrity and security against cyber threats. This approach enhances transaction speed, user convenience, and overall ATM security, reducing reliance on traditional authentication methods.

Advantages of the Proposed System:

1. Eliminates Card-Related Fraud – Fingerprint authentication removes the need for cards, reducing theft and cloning risks.
2. Faster and Secure Transactions – Direct biometric authentication improves transaction efficiency and security.
3. AI-Based Anti-Spoofing Mechanisms – Prevents unauthorized access through fake fingerprints and biometric fraud.

IV. MODULES

Most biometric technology systems operate on universally accepted basic concepts. To register, a user must first sign up for the biometric system.

1. Enrollment:

The process of obtaining, accessing, processing, and storing a user's biometric data in a template format for later use in a biometric system is known as enrolment. After enrolment, additional efforts at identification and verification are made using the template or templates that were developed.

2. Presentation:

During the presenting process, the user enters their biometric data into an acquisition device, which is the hardware in charge of gathering biometric data. Depending on the biometric system, presenting oneself may include repeating a pass phrase, placing a finger on a platen, or looking into a camera.

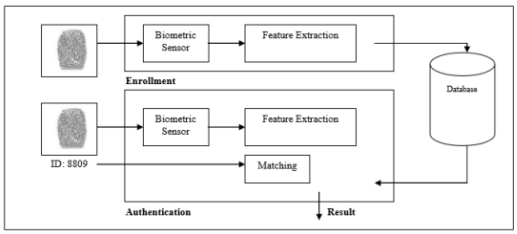
3. Biometric data:

the unprocessed, unaltered image or recording of an individual's biometric information that they supply. The unprocessed data is also known as raw biometric data or biometric samples. Raw biometric data cannot be used for biometric matching. Rather, user information provided during registration and verification is used to create biometric templates, which are thereafter deleted in practically all systems. So Biometric systems use biometric data to generate templates rather than store it. Enrolment requires the creation of a unique identifier, such as an ID or username. The user or administrator frequently creates this identity while submitting personal data. After entering the identify, the user returns to confirm by providing biometric information. Following the collection of biometric data, biometric templates might be created using a feature extraction process.

4. Feature extraction:

Feature extraction is the process of identifying distinctive characteristics in biometric data and automatically encoding them to produce a template. Feature extraction takes place at the

time of registration or verification, or anytime a template is created. Feature extraction includes image and data optimisation and filtering to aid in more accurate feature discovery. For example, fingerprint-scan technologies usually reduce the ridges in a fingerprint image to the width of one pixel, whereas voice-scan technologies frequently filter certain patterns and frequencies. The quality of a biometric system's feature extraction greatly affects its efficiency since it dictates how effectively the system can generate templates.



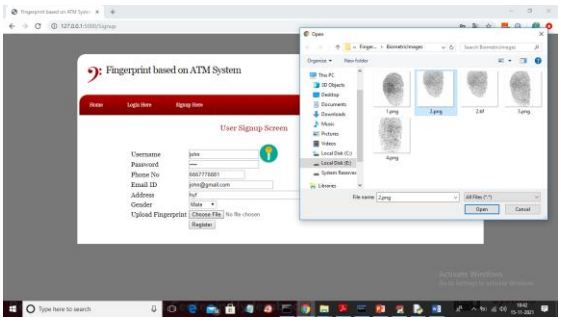
V. OUTPUT

Instead of utilising the user's PIN or password, which is the approach utilised in all other banking applications, we are employing their fingerprint for authentication in our proposed online banking application in order to increase security. We developed the components listed below to complete this project.

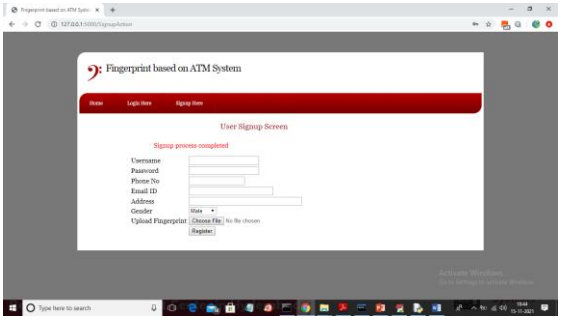
1) **Sign-up:** Using their login, password, and finger print image, users may register for an account and sign up for the application using this module. A MySQL database will house all of the registration data.
2) **Login:** This module allows a user to access the software by entering their username, password, and fingerprint image, which is used to confirm their identification upon registration.
3) **Deposit:** After successful authentication, the user can make a deposit to add funds to his account.
4) **Withdraw:** The user can utilise this to take out the specified amount if there is sufficient balance.
5) **Check Balance:** This module allows the user to check the available balance.

To create a database in MySQL, first copy the contents of "DB.txt" and then paste them into MySQL.

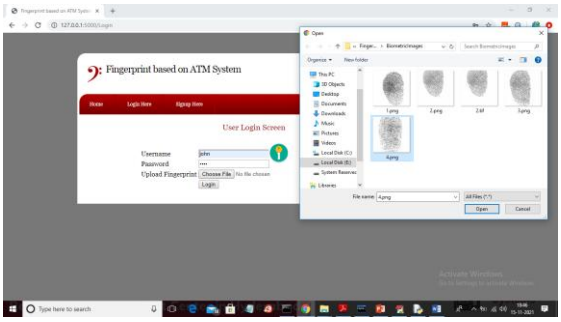
The Python FLASK server for the project is launched by double-clicking the "run.bat" file.



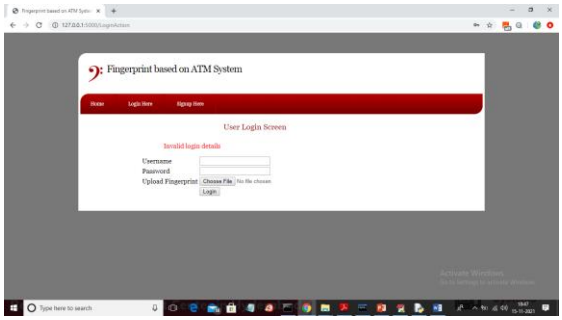
After filling out the registration form on the first page, select the finger print image and click "Open" to view the screen below.



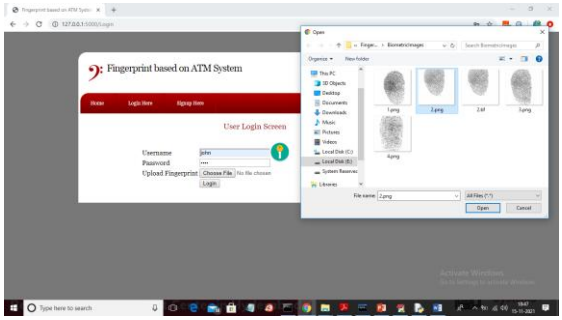
The "Register" button on the page above will be followed by a notification indicating the "Signup process completed." To view the screen below, click the "Login Here" link.



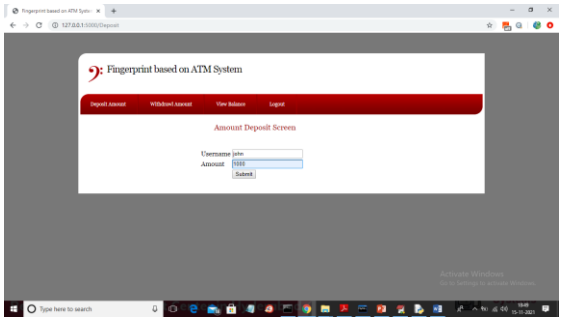
I've chosen the wrong finger print ('4.png') on the page above, and I'm logged in. When the 'Open' button is clicked, the screen below appears.



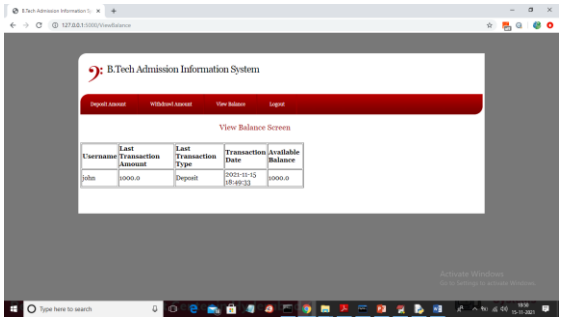
On the screen above, login failed. Please try again with the correct image.



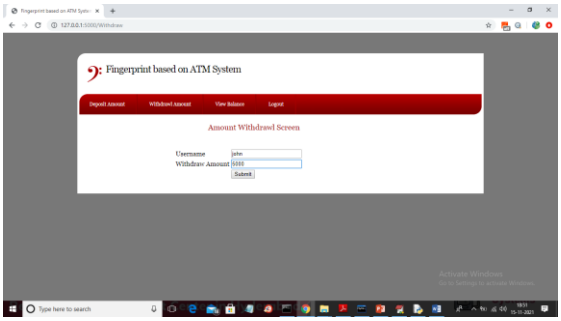
When I click "Login," the result below shows up on the page above where I'm currently uploading the correct image.



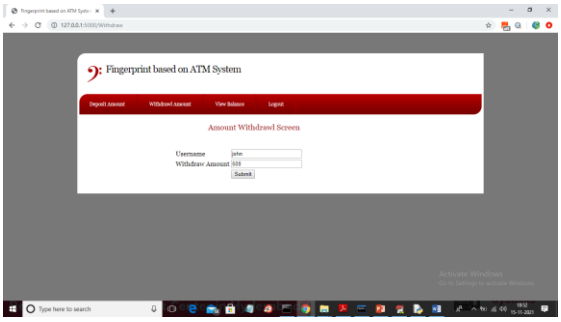
The aforementioned page will immediately display the username. Click "Submit" to complete the transaction after entering the required amount, which will provide the results below.



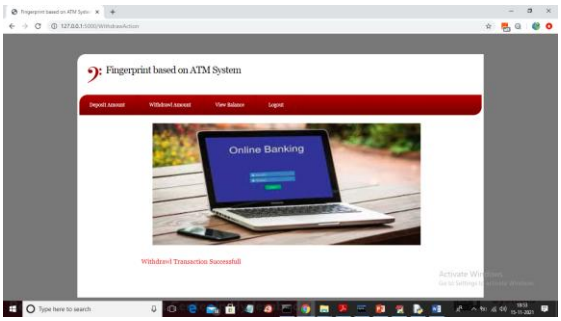
The top page displays the deposit transaction; to view the screen below, click the "Withdrawl Amount" link.



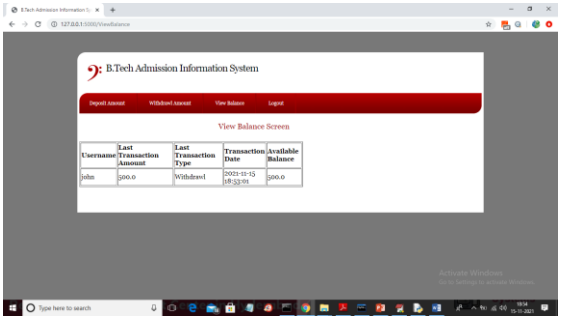
I'm taking out more cash from the screen above than I can get from the screen below.



The screen above shows the withdrawal of $500; click "Submit" to view the screen below.



The withdrawal transaction has been completed on the page above; please check your balance again.



On the screen above, the available balance is now 500. Similarly, you may do N transactions.

VI. VII.CONCLUSION

The increasing vulnerabilities in traditional ATM authentication methods necessitate the adoption of advanced security mechanisms to prevent fraud and unauthorized access. The proposed fingerprint-based biometric authentication system eliminates PIN theft, card skimming, and unauthorized transactions by providing a secure, user-friendly, and efficient alternative to conventional card-based systems. By integrating high-resolution fingerprint scanners, AI-driven anti-spoofing mechanisms, and encrypted biometric databases, the system enhances security, transaction speed, and user convenience. Experimental evaluations demonstrate that biometric authentication significantly reduces fraudulent activities and ensures foolproof access control. This research highlights the importance of biometric security in modern banking systems and sets the foundation for future advancements in AI-driven fraud detection, multi-modal biometric authentication, and decentralized banking security solutions.

FUTURE SCOPE

The implementation of fingerprint-based biometric authentication in ATMs opens up opportunities for further advancements in secure and intelligent banking solutions. Future developments can integrate multi-modal biometric authentication, combining fingerprint recognition with facial recognition or iris scanning for enhanced security. Additionally, AI-driven fraud detection systems can analyze user behavior patterns in real time to detect suspicious activities and prevent unauthorized transactions. The adoption of blockchain technology for secure biometric data storage can further protect user information from cyber threats and unauthorized access. Moreover, cloud-based biometric authentication can enable seamless access to ATMs worldwide, eliminating the need for physical cards across different banking networks. As financial institutions continue to embrace digital transformation, the integration of biometrics with contactless payment systems, mobile banking, and IoT-enabled smart ATMs will revolutionize the way transactions are conducted, making banking more secure, efficient, and fraud-resistant in the future.

REFERENCES

[1] Pranali Ravikant Hatwar and Ravikant B Hatwar, BioSignal based Biometric Practices, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

[2] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, Available at:https://www.sans.org/readingroom/whitepapers/authenticati on/biometric-scanningtechnologies-finger-facial-retinal-scanning-1177.

[3] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37:543-553.

[4] N. Selvaraj and G. Sekar, A Method to enhance the Safety Level of the ATM banking industry using AES Algorithm, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010.

[5] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio networks, Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020. doi:10.1016/jcompeleceng.2020.106784

[6] A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability, Neural Processing Letters, Aug. 2020. doi:10.1007/s11063-020-10327-3

[7] J. Yang N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang A Fingerprint Recognition Scheme supported Assembling Invariant Moments for Cloud Computing Communications, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.

[8] J. Leon G. Sanchez G. Aguilar, L. Toscano, H. Perez and J.M. Ramirez,

Fingerprint Verification Applying Invariant Moments, Proceedings of IEEE International Midwest Symposium on Circuits and Systems, pp. 751-757, 2009.

[9] LO Gorman Overview of Fingerprint Verification Technologies, Information Security Technical Report, Vol. 3, No. 1, p. 21-32, 1998.

[10] G.B. Iwalokun O.C. Akinyokun, B.K. Alese and O. Olabode Fingerprint Image Enhancement: Segmentation to Thinning, International Journal of Advanced computing and Applications,Vol. 3, No. 1, pp. 15-24., 2012.