SURVEY ON ATM SECURITY ENHANCEMENT USING ENCRYPTION TECHNOLOGY

By

HARSHITA PATIL * ROSHANI TALMALE ** SIDDHI YERPUDE ***

RUCHIT PRASAD **** VAIBHAV DHUDAS *****

HARSIMRAN KAUR VIJ ****** TEJAS RAMTEKE *******

*-******* Computer Science and Engineering, S. B. Jain Institute of Technology, Management and Research, Nagpur, India.

https://doi.org/10.26634/jdf.2.2.21234

Date Received: 30/09/2024 Date Revised: 11/10/2024 Date Accepted: 22/10/2024

ABSTRACT

This paper introduces a novel ATM security system that integrates biometric authentication and advanced encryption techniques to enhance safety. The system employs facial recognition and additional biometric methods to strengthen user identification and prevent fraud. It also includes features like helmet or mask detection and one-time password (OTP) authentication to ensure secure transactions. The security framework leverages technologies such as Convolutional Neural Networks (CNNs) and FaceNet for accurate facial recognition. The proposed ATM design includes two levels of security: biometric authentication using a facial image combined with a 4-digit password. Additionally, encryption is reinforced with a wavelet- based Advanced Encryption Standard (AES) algorithm, providing further protection for sensitive information. Future work may explore refining these methods and incorporating additional layers of security to keep up with evolving threats.

Keywords: Enhancement, Biometric Authentication, Security. ATM Vulnerabilities, Cybersecurity, Data Protection, Cryptography.

INTRODUCTION

This study presents a unique approach to enhancing ATM security by integrating biometric authentication with a user-friendly design, setting it apart from broader theoretical works in the field (Vaidya et al., 2018). While much of the existing research focuses on advanced technologies such as Convolutional Neural Networks (CNNs) and multi-biometric systems to combat ATM fraud, this work emphasizes a user-centered solution. Facial recognition technology is combined with traditional verification methods, including the user's full name and PIN, to create an accessible yet secure system that enhances transaction safety (Gyamfi et al., 2016).

What distinguishes this approach is its dual focus on security and usability. Base64 encryption has been implemented to ensure robust protection of sensitive data, and a bilingual interface provides instructional support in both Hindi and English. These features address both technological advancements and the practical needs of a diverse user base, offering written and video instructions to enhance ease of use.

The model emphasizes straightforward and effective security layers, contrasting with studies that focus exclusively on cutting-edge methodologies. By integrating these accessible features into the ATM

ecosystem, this approach delivers a comprehensive, secure, and user-friendly experience tailored to real-world challenges in security and accessibility.

1. Literature Review

Enhancement in ATM Machine Facility Using Face Recognition Security and OTP with Shuffle (More et al., 2023): Automated Teller Machines (ATMs) previously relied on access cards with magnetic stripes and fixed PINs for identity verification, which posed significant security risks. To address these vulnerabilities, researchers proposed a method using a Subscriber Identity Module (SIM) in the user's mobile phone to generate and transmit a PIN to the ATM system. However, this method was found to be susceptible to fraud as the PIN could be intercepted. To further enhance security, the system incorporated face recognition and One-Time Passwords (OTPs) for improved privacy and secure transactions.

Automated Teller Machine Authentication Using Biometric: This study proposed a novel method for secure, card-less ATM authentication by integrating three biometric measures: fingerprint, face, and retina. The system enhanced security and provided robust identification and authorization, effectively reducing the risk of impersonation. The method involved collecting biometric images, converting them to YIQ color space, and applying cellular automata segmentation to extract critical features. Feature extraction was performed using an Enhanced Discrete Wavelet Transform (DWT Mexican Hat Wavelet), followed by multimodal classification through fusion. Machine learning capabilities were improved with an enhanced Deep Convolutional Neural Network (DCNN) combined with a hybrid optimization algorithm, resulting in higher classification accuracy compared to existing algorithms. The research highlighted the potential of biometric technology in reinforcing ATM security and overcoming the limitations of traditional PIN-based systems.

Securing ATM Transactions Using Face Recognition: The study investigated an ATM security enhancement system utilizing facial recognition to prevent unauthorized access and transactions. Technologies such as OpenCV and Local Binary Pattern Histogram were employed for image processing and recognition. The system aimed to verify user identity through facial recognition, reducing the risk of fraudulent activities. Additionally, the literature survey covered diverse related topics, including image steganography, heart disorder prediction, and data privacy protocols, showcasing the breadth of research in technology and security.

Enhanced Security Features of ATMs through Facial Recognition: The research emphasized the significance of Automated Teller Machines (ATMs) in modern banking and highlighted the integration of facial recognition technology with PINs to enhance security. It examined various user scenarios and proposed solutions to reduce ATM-related crimes. The implementation of the Eigenface algorithm for facial comparison was identified as a pivotal feature in strengthening ATM security.

Enhanced Security for ATMs Using Digital Image Processing: This study described a system implemented to improve ATM security by integrating helmet/mask detection, facial recognition, and OTP authentication. It detailed the process flow, algorithmic framework, and potential future improvements in face recognition algorithms. Advanced technologies, including Convolutional Neural Networks (CNN), Multi-task Cascaded Convolutional Networks (MTCNN), FaceNet, and Amazon SNS, were utilized to provide secure and efficient user authentication. The system aimed to enhance security, prevent fraud, and ensure a seamless transaction experience for ATM users.

Biometric-Based ATM Authentication with Wavelet-Based AES Encryption: This paper introduced a secure ATM system that leveraged biometric authentication combined with a wavelet-based AES algorithm. The system ensured dual-layered security by pairing biometric authentication with a 4-digit password at the client side and employing optimized wavelet-based AES encryption for secure communication with the bank server. The integration of biometric measures and a high-speed, low-power AES encryption algorithm significantly improved ATM security.

The study by Vaidya et al. (2016) examined the use of face recognition to enhance ATM security through a verification-based approach.

Table 1 shows the findings from the literature survey, which highlight the key aspects of various ATM security systems. One system incorporated two types of comparison processes: verification, which involved comparing an individual's input with their claimed identity to deliver a "Yes" or "No" decision, and identification, where the system matched the input against all stored identities in the database, generating a ranked list of results. However, the approach had certain drawbacks, including relatively longer processing and verification times for face recognition and the presence of an equal error rate, which limited its effectiveness in specific scenarios.

2. Aim and Objectives

The aim of this work is to enhance the security of ATM systems by integrating advanced technologies such as facial recognition and encryption methods to prevent unauthorized access and fraud. The objective is to strengthen ATM security by integrating facial recognition technology and encryption methods to prevent unauthorized access and fraud. By incorporating these technologies, the system aims to provide an additional layer of security beyond traditional access cards and PINs, ensuring a more secure and reliable ATM experience for users. This approach not only enhances the overall reliability of ATM systems but also protects consumers from identity theft and financial fraud.

3. Overall Review

The collective body of research underscores the critical importance of harnessing advanced technologies, notably facial recognition and biometric authentication, to bolster ATM security while simultaneously enhancing the user experience (Patil et al., 2024). These studies advocate for the adoption of various methodologies aimed at fortifying the existing security measures within ATM systems. Among the proposed approaches are the incorporation of helmet/mask detection systems, the implementation of one-time password (OTP) authentication mechanisms, the utilization of the Eigenface algorithm for facial comparison, and the fusion of multiple biometric modalities including fingerprint, facial, and retinal scans (Mishra et al., 2017).

The ATM systems discussed in these research papers focus on enhancing the security and reliability of Automated Teller Machines (ATMs) using advanced biometric and image processing technologies (Patil et al., 2023). Traditional ATM authentication systems, which rely on bank cards and PINs, are vulnerable to various security threats such as fraud and impersonation. To address these issues, the proposed approaches integrate biometric authentication methods, including fingerprint, facial recognition, and retina scanning, to provide a higher level of security. Additionally, encryption techniques such as Advanced Encryption Standard (AES) are employed to securely store user information and ensure secure communication between the ATM and bank servers (Vaidya et al., 2016).

The primary objective across these studies is to strengthen ATM security by introducing multimodal biometric authentication, ensuring that the system is robust against unauthorized access and fraudulent activities. Furthermore, these systems aim to enhance the overall reliability of ATMs by reducing the dependency on traditional PIN-based methods and introducing more secure and user-friendly alternatives (Joy et al., 2021). The

Paper	Reviews / Findings
Aljuaid and Ansari (2022)	Proposes a card-less ATM authentication system using a fusion of fingerprint, face, and retina biometrics.
Murugesan et al. (2020)	Discusses an ATM security system using facial recognition via OpenCV and Local Binary Pattern Histogram, aiming to reduce fraud through user identity verification.
Peter et al. (2011)	Proposes a face recognition system for ATM verification, highlighting two comparison methods-verification and identification.
Soundari et al. (2021)	Highlights the use of the Eigenface algorithm for facial comparison in ATMs, integrating it with PINs to reduce ATM-related crimes.
Sreedharan (2016)	Combines biometric authentication with wavelet- based AES encryption

Table 1. Findings of Literature Survey

use of advanced algorithms like Deep Convolutional Neural Networks (DCNN), Discrete Wavelet Transform (DWT), and hybrid optimization further contributes to improving the accuracy and efficiency of these systems (Peter et al., 2011).

The overall focus of the papers revolves around enhancing the security of Automated Teller Machine (ATM) systems by integrating advanced biometric authentication methods and digital image processing techniques. These approaches aim to address the limitations of traditional PIN-based systems and prevent unauthorized access and fraud by using technologies such as facial recognition, fingerprint scanning, retina recognition, and cryptographic technique.

4. Proposed Work

The enhanced ATM security system integrates a robust multi-factor authentication process as:

- *Enrollment:* A username, password (PIN), and facial image are provided by users.
- *Withdrawal Process:* The withdrawal option is accessed through the GUI, and facial recognition is undergone by users.
- *Transaction Logging and Security Measures:* User data and communication channels are safeguarded by encryption techniques.
- *Error Handling:* Users are prompted to retry a maximum of three times if inputs and the face do not match.
- *Multimodal Security:* Biometric authentication is combined with other security measures, such as OTPs (One-Time Passwords) and cryptographic techniques, to provide added layers of security.
- *Cryptography:* Advanced Encryption Standard (AES) with wavelet transforms is used to ensure secure communication between ATM machines and banking servers.

This integration significantly reduces the risk of unauthorized access, intrusions, and identity theft, ensuring heightened security for ATM transactions (Hiremath et al., 2020).

5. Existing System

The collective body of research underscores the critical importance of harnessing advanced technologies, notably facial recognition and biometric authentication, to bolster ATM security while simultaneously enhancing the user experience. These studies advocate for the adoption of various methodologies aimed at fortifying the existing security measures within ATM systems. Among the proposed approaches are the incorporation of helmet/mask detection systems, the implementation of one-time password (OTP) authentication mechanisms, the utilization of the Eigenface algorithm for facial comparison, and the fusion of multiple biometric modalities including fingerprint, facial, and retinal scans (Aljuaid & Ansari, 2022).

After the login proces is successful and it is confirmed that the user holds a bank account then the next step will be helmet/scarf detection. If the user is found to be wearing a helmet/scarf the transation process will not continue.For the transaction to continue further the user has to remove the helmet or the scarf and verify his identity (Face recognition). If the entered credentials matches the database of the bank and if the user is not wearing helmet or scarf, then the face recognition takes place.

- Figure 1 shows the login panel. In this system, a login page is used to authenticate whether the user is registered and to verify if their face is uncovered.

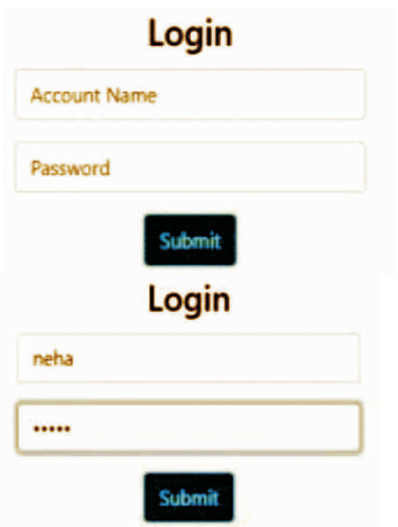

Figure 1. Login Panel

- Figure 2 shows the detection of helmets and scarves. As shown, the system identifies whether an individual is wearing a helmet or covering their face with a scarf.
- This measure could be effective, as many individuals approach ATMs with their faces covered or wearing helmets.

In Another Existing system, the mechanism of two way authentication which provides more security and ensures safe transactions. It includes the use of PIN (Personal Identification Number) which is already provided by the bank, and it is fixed for a specific user (Sreedharan, 2016). Once the PIN gets verified the OTP (One Time password) is generated, which is a randomly generated unique one-time-number (4-6 digit) which is used for providing second factor authentication service which reduces the vulnerabilities of biometric information. The system ensures two times more security compared to the system currently in use and does not require any physical changes to the ATM machines in operation. It also includes OTP features alongside the traditional PIN system, which prevents any criminal from using the ATM card for fraudulent activities. The OTP is valid only once and is sent to the registered mobile number of the owner or customer (Oko & Oruh, 2012). As a result, even if a criminal obtains the PIN, the OTP remains useless, as it changes with every transaction.

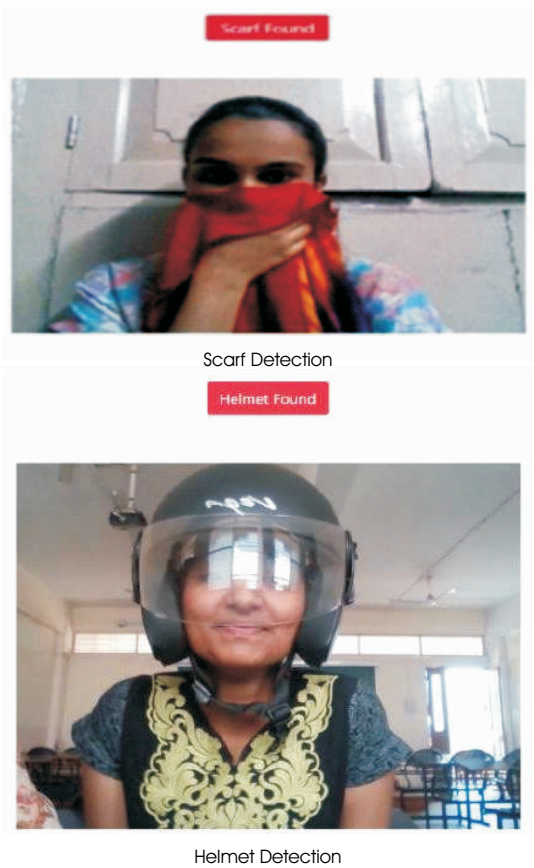

Figure 2. Scarf Detection and Helmet Detection

- *Registration Form:* As shown in Figure 3, the ATM registration form is used to insert data into the database. This form is typically handled by the backend operator or bank personnel and serves purposes such as registering new debit card requests. The form includes mandatory fields such as Name, Phone Number, Email, and PIN. All these fields must be filled out to ensure successful registration.
- *Pin Verification:* The PIN verification process is carried out as shown in Figure 4. When the RFID card is placed near the RFID reader, the card number is automatically displayed in the card number field. The user is then required to enter the 4-digit PIN provided by the bank in the PIN field. To enhance security, the PIN input field features an on-screen randomized numeric keypad, which helps eliminate the risk of PIN tapping and other similar security threats.
- *Withdraw Money:* Once the correct OTP is verified, the two-way authentication process is completed, as shown in Figure 5. At this stage, the user is prompted to enter the desired amount to be withdrawn. This additional layer of security ensures that only authorized transactions are processed.

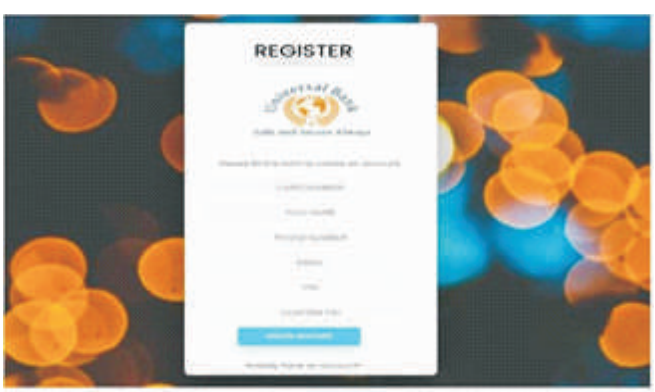

Figure 3. ATM Registration

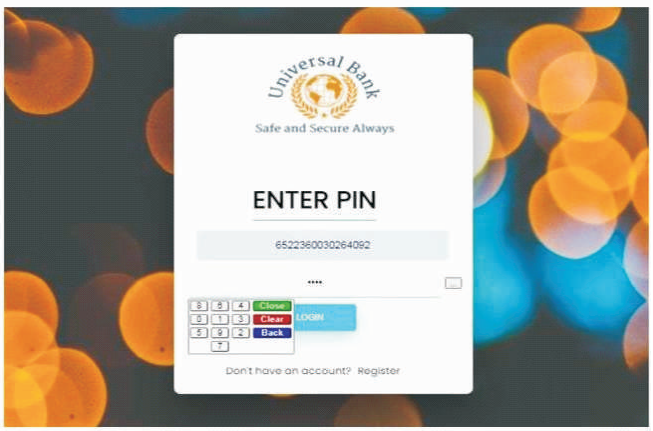

Figure 4. PIN Verification

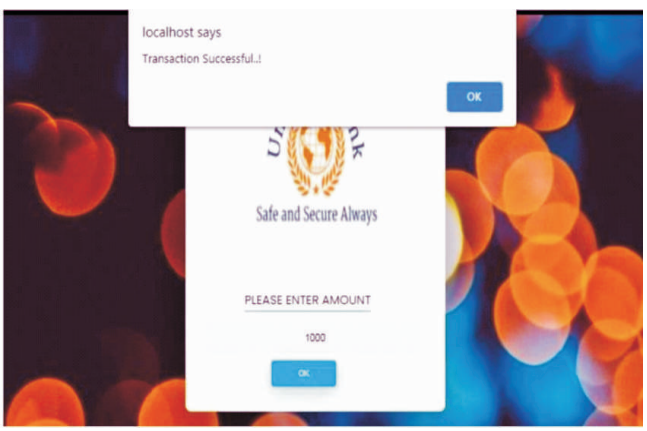

Figure 5. Withdraw Money

6. Existing System Flowchart

The existing system's flowchart, as shown in Figure 6, outlines the step-by-step process of the ATM transaction. It begins with user authentication and proceeds through stages such as PIN verification, account validation, and the withdrawal process. This flowchart highlights the key operations of the current system, ensuring a structured and secure sequence for completing ATM transactions.

- *Start:* The process is initiated when an ATM transaction is started by a user.
- *Take Customer's Picture When Account is Opened:* The customer's picture is captured at the time of opening an account. This image is stored in the bank's database and linked to the customer's account for future verification.
- *At ATM, Use Access Card and PIN to Pre- verify User:* When a transaction is to be performed at the ATM, the access card (ATM card) is inserted, and the PIN (Personal Identification Number) is entered. This step serves as the preliminary verification of the user.
- *If Match is Successful, Allow Transaction Done:* The newly captured image of the user at the ATM is compared by the system to the one stored in the database, taken during account opening. If the images match and the PIN is verified, the verification is deemed successful by the system.

6.1 Decision Point

- *Yes:* If the verification is successful, the process is moved to the next step.
- *No:* If the verification fails (i.e., the images or PIN do not match), the account is suspended by the system to prevent unauthorized access, and the incident is reported to the account holder.
- *Allow Transaction:* After successful verification, the transaction is allowed to proceed. The ATM's services, such as cash withdrawal, become accessible.
- *Card and Cash Retrieval:* The transaction is completed when the card and cash are taken by the user.
- *Stop:* The process is concluded, marking the completion of the transaction.

7. Applications and Advantages

7.1 Applications

- *ATM Security Enhancement:* ATMs can be made more secure through the use of facial recognition and biometric authentication, ensuring more accurate verification of users' identities.
- *Fraud Prevention:* Fraudulent activities at ATMs can be prevented by employing advanced technologies such as helmet/mask detection and one-time passwords, making unauthorized access more difficult.
- *Crime Deterrence:* Criminals can be deterred from targeting ATMs by implementing advanced security measures, potentially reducing the overall incidence of ATM-related crimes
- *Biometric Authentication Systems:* User

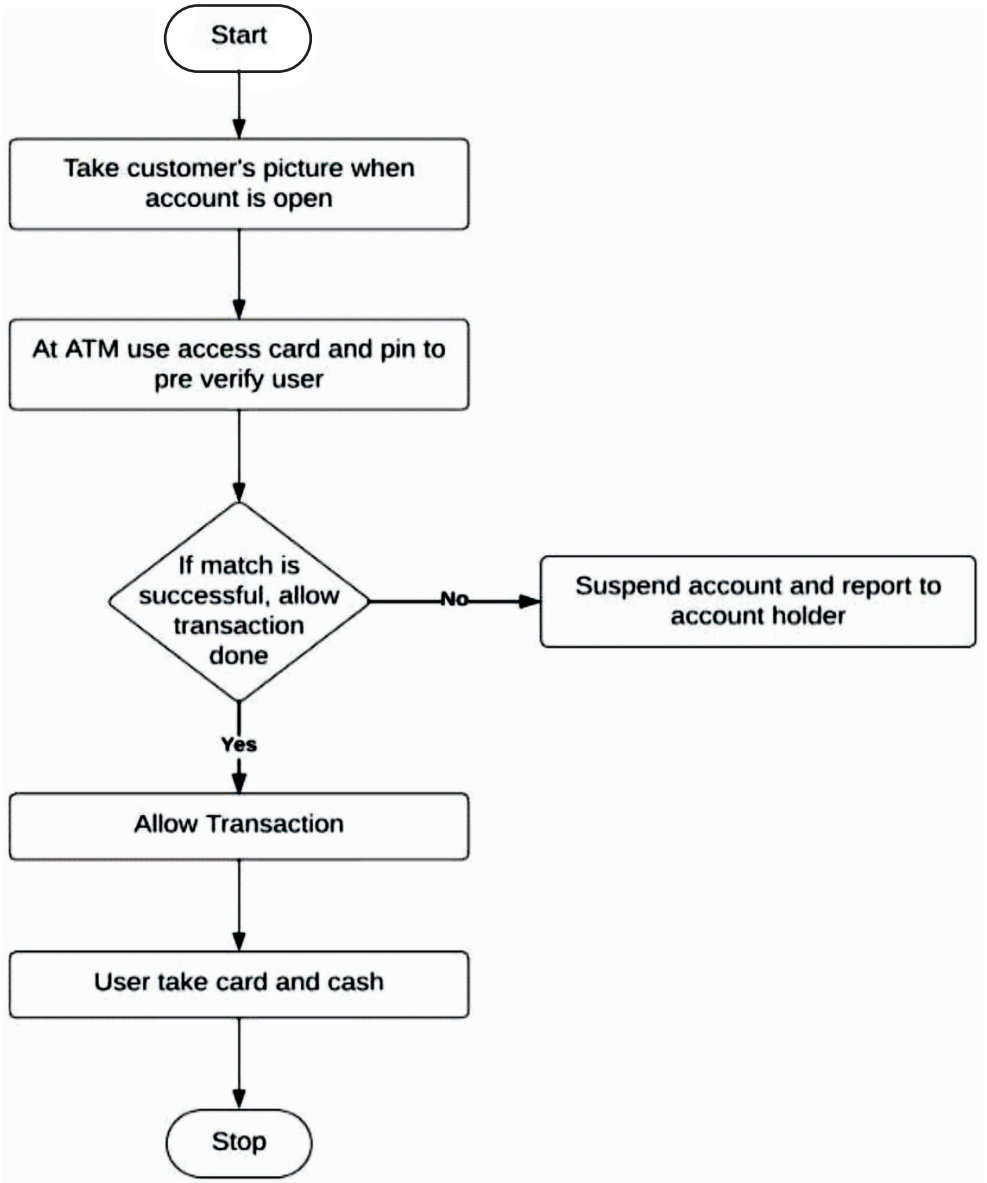

Figure 6. Flowchart for Existing System

authentication is secured in ATMs through fingerprint, facial, and retina recognition.

- *Cryptography-Enhanced ATM Systems:* Secure data transmission between the user and the server is ensured using wavelet-based AES encryption.
- *Multimodal Security Systems:* Multiple biometric and non-biometric security measures are integrated for enhanced security.

7.2 Advantages

- *Enhanced Security:* Multiple security layers, such as facial recognition and biometric authentication, are integrated to significantly enhance ATMs' defense against fraud and unauthorized access.
- *Improved User Experience:* Faster and more secure authentication methods, like facial recognition, are implemented to provide users with a smoother and more convenient ATM experience, resulting in higher satisfaction levels.
- *Increased Trust:* A commitment to state-of-the-art security measures is demonstrated by financial

institutions, instilling greater trust among customers and reassuring them that their transactions are protected and their financial well-being is prioritized.

- *Enhanced Security:* Unauthorized access and fraud risks are significantly reduced through the use of biometric and cryptographic methods.
- *Improved User Experience:* The authentication process is simplified while maintaining higher security levels.
- *Scalability:* These systems are easily adapted to other financial applications or integrated with additional security features, such as QR codes.

Conclusion

This survey highlights the critical advancements in ATM security through the integration of facial recognition, biometric authentication, and robust encryption techniques like the wavelet-based AES algorithm. The studies explored underscore the importance of multi-factor authentication, combining biometric modalities such as fingerprints, retina scans, and facial recognition to establish a more secure framework for ATM transactions. By implementing these cutting-edge technologies, risks such as identity theft, fraud, and unauthorized access can be significantly mitigated. The addition of helmet/mask detection and one-time password (OTP) authentication enhances security by providing multiple layers of protection without compromising user convenience. The application of machine learning algorithms, such as CNNs and FaceNet, has been shown to improve the accuracy and reliability of these systems, ensuring a seamless user experience. These approaches have the potential to revolutionize ATM security, ensuring safer financial transactions and setting a new benchmark for future systems.

This study highlights that incorporating multimodal biometric authentication with advanced encryption methods can substantially reduce ATM-related crimes and foster a more secure and efficient banking environment for users worldwide.

References

[1]. Aljuaid, S. M., & Ansari, A. (2022). Automated teller machine authentication using biometric. *Computer Systems Science and Engineering,* 41(3), 1009-1025. https://doi.org/10.32604/csse.2022.020785

[2]. Gyamfi, N. K., Mohammed, M. A., Nuamah-Gyambra, K., Katsriku, F., & Abdulah, J. D. (2016). Enhancing the security features of automated teller machines (ATMs): A Ghanaian perspective. *International Journal of Applied Science and Technology,* 6(1), 102-111.

[3]. Hiremath, V., Jalihal, N., Gavade, N., & Hannurkar, N. (2020). Enhanced security for ATMs using digital image processing. *International Research Journal of Engineering and Technology,* 7(8), 958-963.

[4]. Joy, A., Babu, C., & Chandy, D. A. (2021, March). Enhanced security mechanism for ATM machines. In *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) 1,* 302-306. IEEE. https://doi.org/10.1109/ICACCS51430.2021.9441861

[5]. Mishra, S., Jain, A., Kumar, S., & Goyal, A. (2017). Enhanced ATM security system using GSM, GPS and biometrics. *International Journal of Engineering and Technical Research,* 7(8), 33-37.

[6]. More, A. S., Kamble, S. A., Bharambe, P. K., Satpute, K. V., & Gajbhare, P. N. (2023). Enhancement in ATM machine facility using face recognition security and OTP with shuffle keyboard. *International Journal for Research in Applied Science and Engineering Technology,* 11(5).

[7]. Murugesan, M., Santhosh, M., Sasiwarman, M., Kumar, T. S., & Valanarasu, I. (2020). Securing ATM transactions using face recognition. *International Journal of Advances in Engineering and Emerging Technology,* 11(2), 52-59. https://doi.org/10.30534/ijatcse/2020/59922020

[8]. Oko, S., & Oruh, J. (2012). Enhanced ATM security system using biometrics. *International Journal of Computer Science (IJCSI),* 9(5), 352-357.

[9]. Patil, H., Wankhede, S., Raut, M., Chimote, E., Thakare, H., Tote, J., & Kundal, A. (2024). IoT-based

collision detection system. *International Research Journal on Advanced Engineering and Management (IRJAEM),* 2(2), 20-26.

https://doi.org/10.47392/IRJAEM.2024.0004

[10]. Patil, H., Wankhede, S., Thakur, S., Pathak, S., Tiwaskar, P., Tembhurne, S., & Sheikh, A. (2023). Object detection models from classical methods to the latest deep learning-based approaches. *Mukt Shabd Journal,* 8(8), 1182-1187.

https://doi.org/10.0014.MSJ.2023.V12I12.0086781.11806

[11]. Peter, K. J., Glory, G. G. S., Arguman, S., Nagarajan, G., Devi, V. S., & Kannan, K. S. (2011, April). Improving ATM security via face recognition. In *2011 3rd International Conference on Electronics Computer Technology,* 6, 373-376. IEEE.

https://doi.org/10.1109/ICECTECH.2011.5942118

[12]. Soundari, D. V., Aravindh, R., & Abishek, S. (2021, May). Enhanced security feature of atm's through facial recognition. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1252-1256). IEEE.

https://doi.org/10.1109/ICICCS51141.2021.9432327

[13]. Sreedharan, A. (2016). Enhanced ATM security using biometric authentication and wavelet based AES. In *MATEC Web of Conferences,* 42, 06003. EDP Sciences.

https://doi.org/10.1051/matecconf/20164206003

[14]. Vaidya, C., Khobragade, P., & Golghate, A. (2016). Data leakage detection and security in cloud computing. *GRD Journals Global Research Development Journal for Engineering,* 1(12), 137-140.

[15]. Vaidya, C., Nampalliwar, A., Nampalliwar, K., Thakkar, R., & Bhagat, S. (2018). Statistical approach for load distribution in decentralized cloud computing. *Helix,* 8(5), 3884-3887.

[16]. Vaidya, C., Takalkar, K., Ghosekar, A., Nimgade, S., & Ghode, V. (2023, February). Decentralized file sharing. In *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1-6). IEEE.

https://doi.org/10.1109/SCEECS57921.2023.10062977

ABOUT THE AUTHORS

Harshita Patil is working as an Assistant Professor at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India.

Roshani Talmale is working as an Assistant Professor at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India.

Sidhhi Yerpude is a Student at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India.

Ruchit Prasad is a Student at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India.

Vaibhv Dhudas is a Student at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India.

Harsimran Kaur Vij is a Student at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India..

Tejas Ramteke is a Student at the S.B. Jain Institute of Technology, Management, and Research, Nagpur, Maharashtra, India.