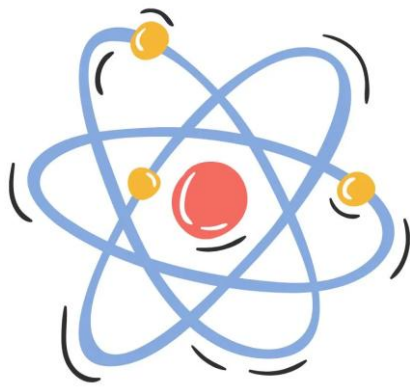




ISSN: 1672 - 6553

JOURNAL OF DYNAMICS AND CONTROL

VOLUME 9 ISSUE 3: 116 - 123

A NOVEL HYBRID MODEL FOR ATM SECURITY USING FACE RECOGNITION AND OTP AUTHENTICATION

Jannet Emimal M.¹, Jayanthi M.²,
Santhi S.³

¹Student, ²Assistant Professor, ³Professor
Department of Computer Science and
Engineering, KIT – Kalaighnar karunanidhi
Institute of Technology, Coimbatore, India

A NOVEL HYBRID MODEL FOR ATM SECURITY USING FACE RECOGNITION AND OTP AUTHENTICATION

Jannet Emimal M.¹, Jayanthi M.², Santhi S.³

¹Student, ²Assistant Professor, ³Professor

Department of Computer Science and Engineering

KIT – Kalaingar karunanidhi Institute of Technology, Coimbatore, India

¹kit.23.19bcs020@gmail.com, ²jayanthikit2020@gmail.com, ³ssanthi.kit@gmail.com

Abstract: An Automated Teller Machine (ATM) is a cash dispensing terminal that allows patrons to conduct financial operations without requiring human assistance, including flows, forfeitures, deposits to be made, and balance inquiries. The security of ATM remains a significant concern, with card skimming, phishing, and unauthorized access being prevalent threats. A wide range of technologies, such as PIN, OTP, biometric, RFID, etc., are used to secure ATM machines. This study presents a survey of various ATM security mechanisms, these technologies have several downsides. The combination of OTP and face recognition technology appears to be superior and more secure than other technologies when compared to other technologies used for ATM security. The integration of these two authentication methods provides a robust defense against various types of attacks, including card cloning, identity theft, and shoulder surfing. The system's usability and user acceptance are also evaluated, showing a positive response from participants. This research contributes to the development of secure and reliable ATM systems, protecting users' financial information and preventing fraudulent activities

Keywords: ATM Security, Face Recognition, One Time Password (OTP), Multimodal Authentication.

1. Introduction

The financial services sector is one of the most significant aspects of a person's daily existence. As banking facilities expanded more quickly, people used it to support their economic endeavors. An automated teller machine, or ATM, is one of the facilities that the bank offers its clients. The ATM was introduced in the year of 1960s. With over 3.5 million ATMs worldwide, these machines have become an essential part of modern banking, offering convenience, speed, and security.

Since crimes committed at ATMs are becoming a major problem, ATM security is becoming an essential concern that needs to be solved. A hacker can quickly take out all of the money once the customer's card has been stolen and their PIN is known. The attackers are more skilled at employing various applications and techniques to breach the ATM system. Therefore, there are several ways to offer security for money withdrawals in order to prevent ATM-related frauds. This study also demonstrates the various approaches that different scholars have taken to address these issues, such as biometrics, PIN generation, and OTP. Despite the fact, OTP with face recognition is more accurate and user-friendly than the others.

Attacks on ATM

1. *Card Skimming:* It is a financial crime occurs when criminals connect equipment to ATMs or card readers in order to obtain private data, such as PINs, CVVs, expiration dates, and card numbers. Skimmers can be external, internal, or overlay, and hidden cameras, glue or tape remnants, and sloppy or uneven card readers are all indicators of manipulation. They instantly deduct the cash from our account after acquiring the details.

2. *ATM Jackpotting*: It is a sophisticated cybercrime where hackers gain unauthorized access to an ATM's internal computer, allowing them to dispense large amounts of cash without using a card or PIN. Usually targeting free standing ATMs in remote locations, thieves take advantage of flaws in ATM software or utilize malware to take over the device. The hacker can empty the ATM's vault by issuing commands to dispense cash once they have gained access. This type of attack sometimes referred to as "logical attacks," can cause banks and other financial organizations to suffer large losses; in certain cases, the damages can reach \$50,000 or more per occurrence.

3. *Malware Attack*: When malicious software is put in ATMs, it can lead to malware infection, which gives hackers access to sensitive data. Usually, thieves take advantage of system flaws or inserts infected USB drives, CDs, or DVDs into the ATM's internal computer. The malware can alter transaction amounts and dispense cash, disable security cameras and alarms, send stolen data to distant sites, and capture card numbers, expiration dates, and PINs once it has been infected.

4. *Black Box Attack*: A Black Box Attack is an assortment of cyber-physical attack in which thieves use an unauthorized device to manipulate an automated teller machine (ATM) and take out cash without a valid bank card. These assaults are now a serious risk to financial institutions around the globe. The target of this attack is to make the protection of an atm security weak or with outdated software

2. Literature Survey

[1] Udhayakumar N, Sri Vasu R, Subhash S, Sharmila Rani D, "ATM-Security using machine learning technique in IOT" In the current endeavor, the taker will only be permitted once if their face has been recognized by the ATM's CCTV camera. The OTP is remit to the enrolled mobile phone, which the user must enter if the authorized user is unable to operate the ATM. Here the main drawback is the authorized person's face can't be recognized if the light setting is bad or he/ she wears an glasses or he may have beard in such cases it fails to recognize the person's face. New modules can be introduced in the future.

[2] Jathumithran S, Thamilarasan V, piratheepan P, Rushanthini P, Mercy veniancy J, Nirupa P, Thiruthanigesan K, "Enhancing ATM Security using Fingerprint" This research is based on implementing the Fingerprint mechanism in the ATM system. Here the user need to be registered his/her Fingerprint during the account open. At first it verifies with the Fingerprint of the user if it matches it asks for the PIN of the account after the verification the user can withdraw the amount. The drawback here is the only authorized person has the access and Fingerprint may change in few years, in some case the Fingerprint may mismatch.

[3] Nongmeikapam Thoiba Singh, Richa Dhiman, Amrita Chaudhary, Prerna Dhawan, Asem Debala Chanu, "Enhancing ATM Security and Convenience with Fingerprint Based Biometric Authentication" To increase the security and usability of the system, finger print recognition technology is employed for both identification and verification. This research offers a succinct examination of the intellectual underpinnings and organizational design of fingerprint recognition. the implementation of biometric authentication in ATM systems, has the potential to revolutionize banking services, offering users a more secure and convenient way to access their funds. Further investigation in this area can fore-front to even more robust and sophisticated biometric authentication systems, ensuring the safety of users' financial transactions.

[6] Rashmi Pte, Sushil Kulkarni, "Securing cash withdrawal fromATM with the help of Smart Mobile Banking Application", Around the world, ATMs are a very significant

instrument. We all utilize ATMs to meet our various banking requirements. We are proposing an ATM withdrawal mechanism that makes use of a Smart Mobile Banking Application. The client must first install the smart mobile banking app from the bank portal and register the smartphone with the bank server. When requesting a cash withdrawal from SMBA, customers can create a password as a security measure. The cash withdrawal is partially committed to the bank's database after it is initiated and the bank server successfully authenticates the password. The customer can then visit the closest ATM and pick up the cash by transferring personal information via a QRC

Table 1. Summary Table

Feature	PIN	Biometric Based	OTP-Based	Token-Based	Face Recognition + OTP
Security	Low	High	Medium	Medium	Very High
Convenience	High	Medium	Medium	Low	High
Implementation Cost	Low	High	Medium	Medium	Medium
Resistance to Spoofing	Low	Medium	Medium	High	Very High
Network Dependency	Low	Low	High	Low	Medium

The comparative analysis of ATM security methods in table 1 highlights the strengths and weaknesses of various approaches, demonstrating the superiority of the proposed system integrating face recognition and OTP. Traditional PIN-based authentication, while simple and cost-effective, is vulnerable to shoulder surfing, card skimming, and PIN theft. Biometric systems, such as fingerprint and iris recognition, offer higher accuracy and security but are susceptible to spoofing and database breaches while also incurring high implementation costs. OTP-based systems provide dynamic, time-sensitive authentication but depend heavily on mobile network reliability and are susceptible to SIM swapping attacks. Token-based systems, like smart cards and key fobs, offer offline security but require users to carry physical devices, which can be lost or stolen. Two-factor authentication (2FA), combining methods like PIN and OTP, improves security but still remains prone to phishing and social engineering attacks. In contrast, the proposed system leverages the unique strengths of both face recognition and OTP, offering robust multi-layered security. Facial recognition ensures secure and convenient biometric verification, with liveness detection to prevent spoofing, while OTP adds a dynamic, time-sensitive layer of protection. Though the system requires initial investment in biometric hardware and relies partially on network availability, it significantly enhances resistance to unauthorized access, card skimming, and PIN theft. The combination of these technologies strikes a balance between high security and user convenience, making it a superior solution for modern ATM security challenges.

3. Existing System

In the existing system, the user will swipe the ATM card and enter the allotted PIN number of that card and this is the traditional method used everywhere, The user inserts the ATM card and enters the PIN if it is correct it goes for an option for face recognition or OTP. It checks for the users face with the already stored image in the database, if it matches it moves to next step to OTP verification where the user needs to type an one-time password which is send to the users mobile phone else shows an warning message.

Drawbacks:

- Card Skimming and Cloning
- Wrong Password or PIN
- Physical Tampering
- Unsecured Network Connections

4. Proposed System

The Enhanced ATM Security using Face Recognition and OTP or MPIN integrates three layers of security to safeguard ATM transactions. The system first analyzes the phone number and account to stored information. It then looks for facial recognition, then if it matches the data that has already been recorded, it moves on to the next step, which involves generating an OTP or MPIN. Its multifactor authentication certify that only authorized patron can flare-up their accounts, reducing the risk of unauthorized transactions, card skimming, and PIN theft. The system's security features include OTP expiration and re-generation, voiceprint encryption, and secure storage, as well as ATM tamper detection and response. By leveraging cutting-edge technologies, it provides a robust and secure ATM security solution that protects users' financial information and complies with regulatory security standards.

5. Working Methodology

The combination of Face Recognition and OTP or MPIN for ATM security enhances the authentication process, adding an extra layer of protection beyond traditional PIN based verification. This methodology aims to ensure that only authorized users can access their accounts, reducing fraud and enhancing user security. Here's a breakdown of how these two technologies work together in an ATM environment and Figure 1 represent the workflow of an ATM.

Step 1: User Registration and Enrollment

- a) *Account Creation:* During the account opening process, the user provides their details, including their facial data (captured via a camera) and preferred authentication method (OTP or MPIN).
- b) *Facial Data Capture:* The user's facial data is collected and stored securely in an encrypted format within the bank's database.
- c) *MPIN/OTP Setup:*
- **MPIN:** The user sets a secure, memorable 4 – 6 digit MPIN.
 - **OTP:** The system links the user's mobile number to send OTPs during transactions.
- d) *Data Synchronization:* All the above information is linked to the user's bank account and ATM card.

Step 2: ATM Authentication Process**1. ATM Card or Cardless Entry:**

- **With Card:** The user inserts their ATM card into the machine.

- Cardless Option: The system prompts the user to enter their account number or scan a QR code.

2. Face Recognition

- The ATM system activates a camera to capture the user's facial image.
- The captured image is matched against the facial data stored in the bank's secure database using advanced face recognition algorithms.
- If the match fails, the system denies access.

Step 3: Secondary Authentication

- Choose Authentication Mode:

If face recognition is successful, the system prompts the user to authenticate via OTP or MPIN.

- OTP Authentication:

The system sends a one-time password (OTP) to the registered mobile number. The user enters the OTP on the ATM.

a) MPIN Authentication:

The user enters their predefined MPIN on the ATM keypad.

b) Verification

The system validates the OTP or MPIN entered by the user. If the entered value is incorrect, the transaction is blocked, and the user is notified.

Step 4: Transaction Processing

a) Access Granted:

If both facial recognition and secondary authentication are successful, the user is granted access to the ATM functions.

b) Transaction Execution:

The user selects the desired service (withdrawal, deposit, balance inquiry, etc.). The transaction is processed securely.

Step 5: Post-Transaction Processing

a) Session Termination:

After the transaction, the system automatically logs the user out to prevent unauthorized access.

b) Notification:

The user receives a transaction confirmation via SMS or email.

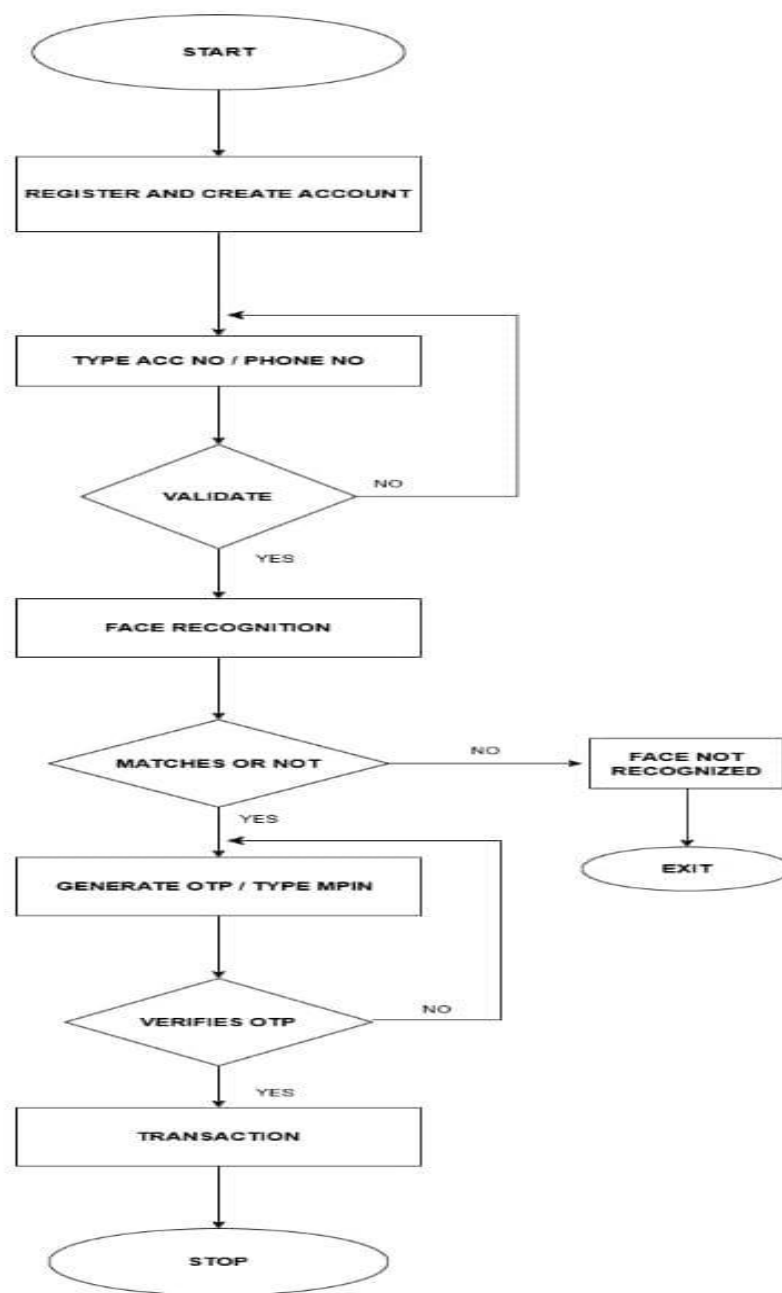


Figure 1. Workflow of an ATM

6. Result and Analysis

The experimental results demonstrate that the proposed system combining facial recognition and OTP provides a highly secure and efficient solution for ATM transactions. The system's robust authentication mechanisms ensure that only authorized users gain access while maintaining a user-friendly experience. Although challenges such as low-light conditions and network dependency were identified, these can be mitigated through system enhancements. The overall performance in

Figure 2 indicates that this system significantly improves ATM security, aligning with modern standards and user expectations.

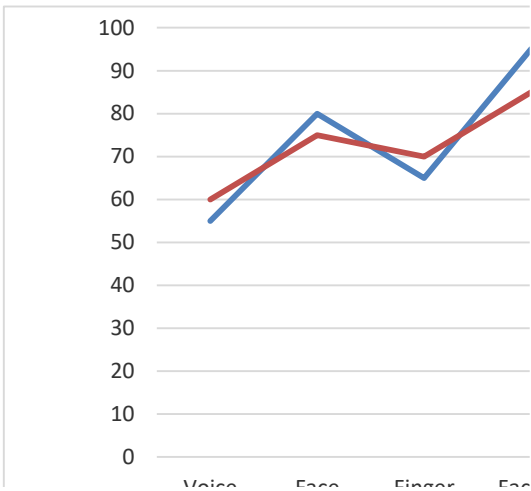


Figure 1. Comparison of Proposed Architecture with the Existing Architecture

A summary of the accuracy and effectiveness of various authentication techniques is illustrated in Figure 2. The accuracy and efficiency of voice-based authentication are the lowest. Compared to voice, face recognition exhibits a notable gain, peaking and then somewhat falling. Both accuracy and efficiency are maintained with fingerprint authentication. The greatest accuracy and efficiency are attained by Face & OTP authentication, demonstrating its superiority over alternative techniques. This comparison shows that the suggested architecture, which uses Face & OTP, offers the best security solution because it is more accurate and efficient than conventional techniques.

Table 1. Result Summary

Metric	Result
Facial Recognition Accuracy	95%
Liveness Detection Success Rate	98%
OTP Delivery Success Rate	99%
Average OTP Delivery Time	5 seconds
Average Transaction Time	45 seconds
User Satisfaction Rate	90%

8. Conclusion

In conclusion, integrating Face Recognition and OTP or MPIN into ATM security represents a significant advancement in safeguarding financial transactions. By combining two-factor authentication through OTP sent to users’ mobile phones and biometric verification via Face recognition, this approach enhances security by making it much harder for unauthorized individuals to access ATM services. While OTP provides an additional layer of dynamic authentication, Face recognition leverages the unique facial characteristics of the user, ensuring that even if one factor is compromised, the other remains a strong

barrier against fraud. The Accuracy and Efficiency of the project is shown in the Figure 2 and the result summary of our work is mentioned in Table 2. This dual authentication method minimizes the risks associated with traditional PIN-based systems, which are vulnerable to skimming and theft.

Acknowledgments

I would like to express their sincere gratitude to Kalaikarunanidhi Institute of Technology for providing the necessary resources and support throughout this research. We extend our appreciation to Ms.M.Jayanthi and Ms.S.Santhi for their insightful discussions and valuable feedback. Additionally, we acknowledge there is no financial support. Lastly, we thank the editorial team and reviewers of the *Journal of Dynamic and Control* for their time and constructive comments, which have helped improve the quality of this paper.

9. References

9.1. Journal Article

- [1] Udhayakumar N, Sri Vasu R, Subhash S, Sharmila Rani D, "ATM-Security using machine learning technique in IOT" in International Journal of Advance Research Ideas and Innovations in Technology, 2022.
- [2] Jathumithran S, Thamilarasan V, piratheepan P, Rushanthini P, Mercy veniancy J, Nirupa P, Thiruthanigesan K, " Enhancing ATM Security using Fingerprint " in ICTACT Journal on Micro Electronics, 2018.
- [3] Nongmeikapam Thoiba Singh, Richa Dhiman, Amrita Chaudhary, Prerna Dhawan, Asem Debala Chanu, "Enhancing ATM Security and Convenience with Fingerprint-Based Biometric Authentication" in Research gate, 2024.
- [4] Mr. Abhinay G. Dhamankar, Trupti Khade, Prashant Patil, Manish Raut, Shashank Satghare, "Enhancing ATM security using Face Recognition" in International Research Journal of Modernization in Engineering Technology and Science, 2023
- [5] Sonal Mahajan, Anagha Awale, Rutuja Gurav, Pranjal Satpute, Ms. Hema Karande, Mr. Jitendra Bakliwal, "Cardless transaction in ATM" in IJRASET Journal For Research in Applied Science and Engineering Technology, 2023.
- [6] Sahil Bajaj, Sumit Dawda, Pradnya Jadhav, Rasika Shirude, "Card less ATM Using Deep Learning and Facial Recognition Features", in Journal of Information Technology and Software Engineering, 2022.
- [7] Surawse, P., Bhange, Taru, S., Khot, S., & Mundada, Prof. J "Secure ATM Transactions Using Face Recognition & OTP", in JETIR February, 2022.

9.2. Conference Proceedings

- [8] Rashmi Pte, Sushil Kulkarni, "Securing cash withdrawal from ATM with the help of Smart Mobile Banking Application" in International Conference on Interdisciplinary Research in Technology & Management, 2022.
- [9] M. T. H. Fuad et al., "Recent Advances in Deep Learning Techniques for Face Recognition", in IEEE, 2021
- [10] K.Yadav, S. Mattas, L. Saini and P. Jindal, "Secure Card-less ATM Transactions," in First IEEE International Conference on Measurement, Instrumentation, Control and Automation, 2020.
- [11] P. Choudhary, A. Tripathi, A.K. Singh and P.C. Vashist, "Implementation of integrated security system by using biometric function in ATM machine" in Intelligent Computing in Engineering: Select Proceedings of RICE 2020,
- [12] Ashwini M Zinjurde, Vilas B Kamble, "Credit Card Fraud Detection And Prevention By Face Recognition", in IEEE, 2020.
- [13] S. Takkar, M. Rakhra, A. Ratnani, D.S. Protyay, P. Pandey and M. Arora, "Advanced ATM security system using Arduino Uno", in 9th International Conference on Reliability", Infocom Technologies and Optimization, 2021.
- [14] Mohsin Karvaliyaa , Saifali Karediab , Sharad Ozac , Dr.D.R Kalbanded "Enhanced security for ATM machine with OTP and Facial recognition features" in International Conference on Advanced Computing Technologies and Applications Elsevier, 2015.