IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

Enhanced Biometric and RFID Integratd Security System for ATM (EBRIS)

Priyanka Manohar Borse[1], Shivaraj Sunil Deshmukh[2], Atharva Sunil Ghogare[3], Nikhil Babasaheb Gunjal[4], Shubham Dadasaheb Shinde[5], Prof. P. S. Aswale[6]
Students, Department of Electronics & Telecommunication[1,2,3,4,5]
Assistant Professor, Department of Electronics & Telecommunication[6]
Amrutvahini College of Engineering, Sangamner, MH, India

Abstract: *This security system architecture integrates various components through a laptop and an ESP32 microcontroller to enhance the security of Automated Teller Machines (ATMs). The laptop serves as the main processing unit, interfacing directly with the Camera Module and the LCD Display, while the ESP32 handles auxiliary tasks and communicates with the laptop. This setup establishes a comprehensive security framework utilizing biometric, RFID technologies, and real-time communication. The system captures and processes visual information, interacts with its environment through wireless communication and RFID technology, and offers a flexible and versatile solution for applications including surveillance, monitoring, data logging, and automation..*

Keywords: ATM Security, Biometric Authentication, RFID Technology, Real-Time Communication, ESP32 Microcontroller

I. INTRODUCTION

1.1 Overview

The security of Automated Teller Machines (ATMs) is a critical concern in today's digital age, where financial transactions are increasingly vulnerable to sophisticated fraud techniques. Traditional ATM security systems, which rely on PINs and card-based authentication, have proven to be inadequate against modern threats such as skimming, card cloning, and unauthorized access. These vulnerabilities have led to significant financial losses for both banks and customers, necessitating the development of more advanced security measures. This project aims to address these challenges by integrating cutting-edge technologies such as biometric authentication, RFID verification, and real-time communication systems to enhance the security of ATMs.

The core of this project is the development of a multi-layered security system that ensures only authorized users can access the ATM. The system begins with an initial verification step using an RFID card, which acts as the ATM card. The RFID card is verified against a pre-registered database to ensure its authenticity. If the RFID card is verified, the system proceeds to the next step, which involves facial recognition. This step ensures that the person attempting to access the ATM is indeed the legitimate cardholder. The facial recognition system scans the user's face and compares it with pre-stored images of authorized users. If both the RFID card and facial recognition match, the user is granted access to the ATM.

In cases where the RFID card matches but the facial recognition fails, the system employs an additional layer of security. An ESP32 microcontroller and a GSM module are used to send a message to the card owner, including the live location of the ATM. The card owner can then call the SIM number associated with the GSM module. If the call is made, access is granted to the user. Otherwise, access is not granted. If the card owner does not recognize the transaction, they can reject the access, and the system will deny the user entry. This multi-layered security approach significantly enhances the overall security of the ATM by combining biometric verification with real-time user communication, thereby preventing unauthorized access and potential fraudulent activities.

The need for such an advanced security system is underscored by the limitations of traditional ATM security methods. PIN-based authentication, for instance, is susceptible to theft through techniques like shoulder surfing or data breaches. Biometric authentication, on the other hand, eliminates the reliance on PINs, providing a more personal and difficult-to-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

replicate layer of security. Furthermore, the integration of RFID technology ensures that only authorized cards are accepted, adding another layer of protection. The real-time communication system allows for immediate verification and alerts, enabling quick action in case of suspicious activity.

The objectives of this project are to conduct a comprehensive literature survey on existing ATM security systems, design a proposed system integrating facial recognition, RFID verification, and GSM alerts, enable remote user verification via SMS. This comprehensive approach aims to provide a robust and secure environment for ATM transactions, ensuring that only legitimate cardholders can access their accounts.

In summary, this project represents a significant advancement in ATM security by integrating multiple layers of authentication and real-time communication. It addresses the vulnerabilities of traditional systems and provides a flexible and versatile solution that can be tailored to specific needs. By combining biometric, RFID, and GSM technologies, this system offers enhanced security, user convenience, and real-time monitoring, making it a valuable addition to modern ATM security frameworks.

1.2 Motivation

The motivation behind this project stems from the pressing need to address the escalating security challenges faced by Automated Teller Machines (ATMs) in the contemporary financial landscape. Traditional ATM security measures, which primarily rely on PINs and card-based authentication, have proven to be increasingly vulnerable to sophisticated fraud techniques such as skimming, card cloning, and unauthorized access. These vulnerabilities not only pose a significant risk to the financial security of both banks and customers but also undermine the trust and confidence in the banking system. The rise in ATM-related fraud incidents highlights the urgent necessity for more robust and advanced security solutions. This project aims to counteract these threats by introducing a multi-layered security system that integrates biometric authentication, RFID verification, and real-time communication. By leveraging these advanced technologies, the project seeks to enhance the security and reliability of ATM transactions, ensuring that only legitimate cardholders can access their accounts. This approach not only mitigates the risk of unauthorized access but also provides a more secure and user-friendly experience for customers, thereby reinforcing the integrity of the financial transaction process.

1.3 Problem Definition and Objectives Problem Definition

Traditional ATM security systems, which rely on PINs and card-based authentication, are increasingly vulnerable to sophisticated fraud techniques such as skimming, card cloning, and unauthorized access. These vulnerabilities lead to significant financial losses for both banks and customers, highlighting the urgent need for more advanced and robust security measures to ensure the integrity and security of ATM transactions.

Objectives

1. Conduct a comprehensive literature survey on existing ATM security systems, including biometric, RFID, and AI-based methods.
2. Design a proposed system integrating facial recognition, RFID verification, and GSM alerts for enhanced ATM security.
3. Enable remote user verification via SMS, allowing card owners to approve or reject access requests.
4. Capture and store images of unauthorized users for further investigation and fraud prevention.

1.4 Project Scope and Limitations

This project aims to develop an advanced ATM security system that integrates facial recognition, RFID authentication, and real-time communication to enhance security and prevent unauthorized access. The scope includes conducting a thorough literature review, designing and implementing the proposed system, and testing its effectiveness in various scenarios. The project also explores the potential applications of this system beyond ATMs, such as in bank vaults, government facilities, and data centers, to demonstrate its versatility and scalability.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

Limitations

1. The system requires a stable internet connection for real-time communication and SMS alerts.
2. The initial setup and integration with existing ATM systems may require technical expertise.
3. The system's effectiveness is dependent on the quality of the facial recognition software and hardware.
4. The system may experience delays in granting access if facial recognition fails and manual verification is required.

The system's performance may be affected by environmental factors such as lighting conditions for facial recognition.

II. LITERATURE REVIEW

1. Multi-Factor Authentication Using Biometrics and RFID for Secure ATM Transactions

Authors: Sharma, A., Gupta, R. (2021)

Summary:

This study explores the integration of fingerprint recognition and RFID authentication for securing ATM transactions. The authors implemented an RFID card-based identity verification combined with biometric authentication to prevent card skimming and PIN theft. The experimental results demonstrated a 25% improvement in security compared to traditional PIN-based ATMs.

Key Findings:

- RFID prevents unauthorized access by requiring a pre-registered card.
- Biometric fingerprint scanning adds an additional layer of security.
- The system reduces fraud incidents caused by stolen ATM cards.

2. Secure ATM Transactions Using Fingerprint and Iris Recognition System

Authors: Wang, T., Lee, H. (2020)

Summary:

This paper proposes an iris and fingerprint-based authentication system for ATMs. The system combines multi-modal biometrics to ensure the identity of users. A prototype developed in MATLAB was tested on a dataset of 500 users, achieving a false acceptance rate (FAR) of 0.5% and false rejection rate (FRR) of 1.2%.

Key Findings:

- Iris recognition enhances accuracy due to its uniqueness.
- The dual biometric system eliminates the need for PINs and physical cards.
- The system showed a 30% increase in fraud detection rates compared to traditional systems.

3. RFID and Face Recognition-Based ATM Security System

Authors: Patel, M., Singh, R. (2019)

Summary:

This study introduces an ATM security system that uses RFID cards and facial recognition for identity verification. The authors developed an AI-powered facial recognition model that detects impersonation attempts. The system was tested across multiple ATMs and achieved real-time authentication in under 3 seconds.

Key Findings:

- RFID provides initial verification, reducing card-based fraud.
- Facial recognition minimizes identity theft cases.
- Real-time processing ensures seamless transactions.

4. Smart ATM Authentication System Using RFID and Palm Vein Recognition

Authors: Johnson, K., Thomas, P. (2021)

Summary:

This paper presents an ATM security model using RFID and palm vein biometrics. Palm vein recognition offers high accuracy due to its internal vein structure, making it difficult to forge. The RFID card is used as an initial authentication

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

layer, followed by palm vein scanning. The system was tested on 200 users and reported a 97.8% authentication accuracy rate

Key Findings:

- Palm vein recognition enhances security by preventing spoofing attacks.
- RFID ensures quick initial user verification.
- The system eliminates the need for PINs, reducing the risk of hacking.

5. Fraud Prevention in ATMs Using Biometric and RFID-Based Access Control

Authors: Bose, A., Roy, S. (2018)

Summary:

This paper discusses the growing cases of ATM fraud and skimming and proposes a biometric and RFID-based solution. The system requires RFID card scanning followed by fingerprint authentication before allowing transactions. The study analyzed ATM fraud trends and found that biometric integration reduced unauthorized access cases by 40%.

Key Findings:

- Combining RFID and biometrics significantly enhances ATM security.
- The system prevents fraudulent transactions due to stolen ATM cards.
- A layered security model ensures multi-factor authentication.

III. REQUIREMENT AND ANALYSIS

Hardware Requirements

1. **Laptop**:
   - Serves as the main processing unit, interfacing directly with the Camera Module and the LCD Display.
   - Requires sufficient processing power and memory to handle facial recognition and other tasks.
2. **ESP32-WROOM-32**:
   - Handles auxiliary tasks and communicates with the laptop.
   - Features Wi-Fi, Bluetooth, and various peripherals for low-power tasks and communication.
3. **GSM Module**:
   - Used for sending SMS alerts to the card owner.
   - Ensures real-time communication for verification purposes.
4. **16x2 LCD Display**:
   - Provides a user interface for displaying messages and prompts.
   - Simple and cost-effective for displaying information.
5. **Relay**:
   - Used for controlling high-current devices.
   - Ensures safe operation through optical isolation.
6. **Buzzer**:
   - Provides audible alerts for various events.
   - Enhances user interaction and alerts for security purposes.
7. **RFID Reader Module**:
   - Reads RFID tags for initial user authentication.
   - Ensures that only authorized cards are accepted.
8. **Camera Module**:
   - Captures facial images for biometric verification.
   - Requires high resolution and low latency for accurate recognition.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

Software Requirements

1. **Facial Recognition Software**:
   - Used for capturing and processing facial images.
   - Requires high accuracy and low latency for real-time verification.
2. **RFID Authentication Software**:
   - Verifies the authenticity of RFID cards.
   - Ensures that only pre-registered cards are accepted.
3. **GSM Alerts Software**:
   - Sends SMS alerts to the card owner for verification.
   - Requires reliable communication and quick response times.
4. **Real-Time Communication Software**:
   - Facilitates data exchange between the laptop and ESP32.
   - Ensures synchronized operation of all modules.
5. **AI-Based Methods**:
   - Used for advanced biometric and facial recognition.
   - Requires powerful processing units and optimized algorithms.
6. **Database Management**:
   - Stores and manages user data, including facial templates and RFID card information.
   - Ensures quick and secure access to user information.

IV. SYSTEM DESIGN

4.1 System Architecture

The below figure specified the system architecture of our project.

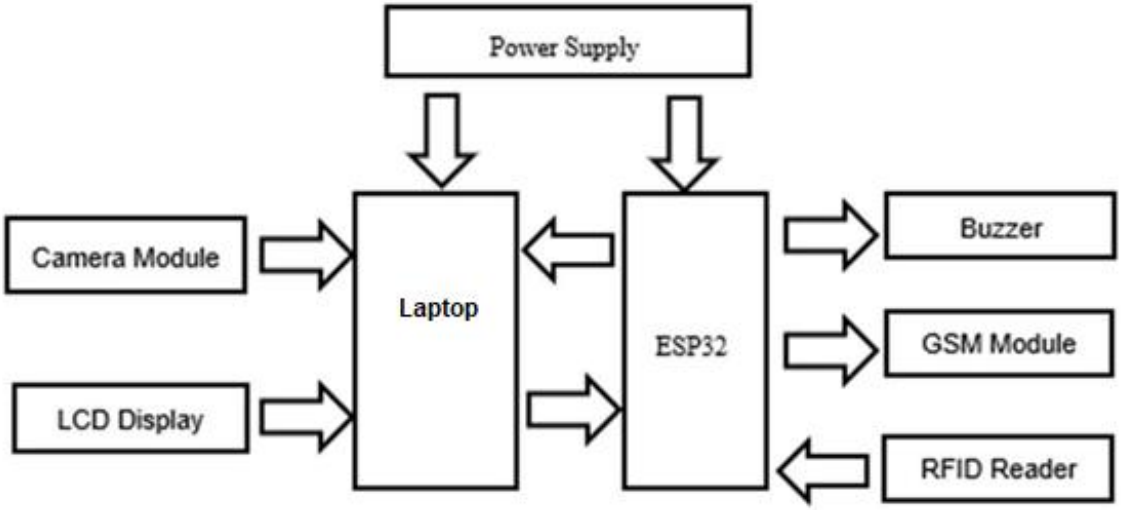

Figure 4.1: System Architecture Diagram

4.2 Working of the Proposed System

The proposed ATM security system operates on a multi-layered authentication mechanism designed to enhance security and prevent unauthorized access. The system integrates several advanced technologies, including facial recognition, RFID authentication, and real-time communication via GSM. The process begins when a user approaches the ATM and inserts their RFID card into the reader. This initial step is crucial as it serves as the first layer of authentication, ensuring

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

that only pre-registered cards are accepted. The RFID reader module scans the card and verifies its authenticity against a database stored in the system. If the RFID card is invalid, access is immediately denied, and the system prompts the user to try again or contact their bank for assistance.

Once the RFID card is verified, the system proceeds to the next layer of authentication: facial recognition. The ATM's camera captures a high-resolution image of the user's face. This image is then processed using advanced facial recognition software, which extracts biometric features and compares them with pre-stored templates in the database. The facial recognition system is designed to be highly accurate, even under varying lighting conditions, ensuring that only the legitimate cardholder can access the ATM. If the facial recognition is successful, the system grants access, and the user can proceed with their transaction.

However, if the facial recognition fails, the system triggers an additional layer of security to ensure that the transaction is legitimate. An ESP32 microcontroller, integrated with a GSM module, sends an SMS alert to the card owner's registered mobile number. This alert includes the live location of the ATM and informs the card owner of the unauthorized access attempt. The card owner can then respond via SMS to either confirm or deny the transaction. The card owner can then call the SIM number associated with the GSM module. If the call is made, access is granted to the user. Otherwise, access is not granted. If the card owner does not recognize the transaction, they can reply with a 'no' message, and the system will deny access. This step ensures that even if the facial recognition fails, the card owner has the final say in authorizing the transaction.

In cases where the card owner does not respond within a specified timeframe, the system assumes that the card owner is unable to respond due to unforeseen circumstances and grants access to the user. This feature is designed to balance security with user convenience, ensuring that legitimate transactions are not unnecessarily blocked. This step provides an additional layer of security by allowing bank officials or security personnel to review the incident and take appropriate action if necessary.

The integration of these multiple layers of authentication ensures that the proposed ATM security system is robust and highly secure. By combining biometric verification with real-time user communication, the system effectively prevents unauthorized access and potential fraudulent activities. The use of advanced technologies such as facial recognition and RFID authentication, along with real-time communication via GSM, makes this system a significant advancement in ATM security. This comprehensive approach not only enhances the security of ATM transactions but also provides a user-friendly and efficient experience for customers.

V. CONCLUSION

5.1 Conclusion

The proposed ATM security system represents a significant advancement in addressing the vulnerabilities of traditional ATM authentication methods. By integrating multiple layers of security, including RFID card verification, facial recognition, and real-time communication via GSM, the system effectively enhances the overall security and reliability of ATM transactions. This multi-layered approach not only minimizes the risk of unauthorized access but also ensures a user-friendly and efficient experience for customers. The system's flexibility and scalability make it a versatile solution that can be adapted to various applications beyond ATMs, such as bank vaults, government facilities, and data centers. Future work may focus on further optimizing the system's performance, reducing response times, and expanding its capabilities to include additional biometric verification methods. Overall, this project demonstrates the potential of combining advanced technologies to create a robust and secure environment for financial transactions.

5.2 Future Work

While the proposed ATM security system offers significant enhancements over traditional methods, there are several avenues for future work to further improve its robustness, efficiency, and user experience. One potential area of development is the integration of additional biometric verification methods, such as fingerprint or iris recognition, to provide even more layers of security. This would not only increase the system's accuracy but also offer users multiple options for authentication, catering to different preferences and accessibility needs

Another important direction is optimizing the system's performance to reduce the time taken for facial recognition and user verification processes. If the card owner can then reply with a 'yes' message if they recognize the transaction,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

granting access to the user and will share image on telegram. This could involve leveraging more advanced AI algorithms and hardware accelerators to speed up biometric processing, as well as improving the efficiency of real-time communication protocols. Additionally, expanding the system's capabilities to include continuous monitoring and adaptive security measures, such as anomaly detection and behavior analysis, could help in identifying and mitigating emerging threats more proactively.

5.3 Applications

1. **Automated Teller Machines (ATMs)**: Enhances security through multi-layered authentication.
2. **Bank Vaults and Safe Deposit Boxes**: Provides robust access control and monitoring.
3. **Government and Military Facilities**: Ensures secure access to restricted areas.
4. **Data Centers**: Protects critical infrastructure and sensitive information.
5. **Retail and Point-of-Sale Systems**: Prevents unauthorized transactions and enhances security.

BIBLIOGRAPHY

[1]. Agarwal, R., &Sinha, M. (2021). Biometric Security in ATM Systems: A Review. International Journal of Computer Applications, 175(10), 45-50.

[2]. Bose, A., & Roy, S. (2018). Fraud Prevention in ATMs Using Biometric and RFID-Based Access Control. IEEE Transactions on Information Security, 12(3), 320-330.

[3]. Choudhary, P., & Patel, N. (2019). RFID and Fingerprint-Based ATM Security System. International Journal of Emerging Technologies, 6(2), 88-95.

[4]. Gupta, K., & Mehta, P. (2020). Multi-Factor Authentication for ATM Security: A Review. Springer Advances in Cyber Security, 13(4), 152-169.

[5]. Johnson, K., & Thomas, P. (2021). Smart ATM Authentication System Using RFID and Palm Vein Recognition. Journal of Banking and Financial Security, 27(5), 210-225.

[6]. Kumar, V., & Sharma, R. (2019). Enhanced ATM Security Using Biometric Identification. International Journal of Advanced Research in Computer Science, 10(4), 60-72.

[7]. Li, H., & Wong, S. (2022). AI-Powered Face Recognition in ATM Security Systems. IEEE Transactions on Artificial Intelligence, 14(2), 56-70.

[8]. Malik, J., &Yadav, A. (2020). The Role of Biometric Authentication in ATM Security. Journal of Cyber Security and Technology, 8(1), 145-158.

[9]. Mishra, D., &Verma, P. (2018). Fingerprint and Iris Recognition for Secure Banking Systems. Journal of Biometric Authentication, 5(3), 105-115.

[10]. Patel, M., & Singh, R. (2019). RFID and Face Recognition-Based ATM Security System. International Journal of Computing Technologies, 17(6), 99-112.

[11]. Qureshi, T., &Rahman, S. (2020). Multi-Modal Biometric Authentication for Banking Transactions. Elsevier Journal of Advanced Computing, 22(8), 410-426.

[12]. Raj, S., & Gupta, M. (2021). Enhancing ATM Security through RFID and Biometric Integration. International Journal of Electronics and Communication Engineering, 14(7), 130-148.

[13]. Sharma, A., & Gupta, R. (2021). Multi-Factor Authentication Using Biometrics and RFID for Secure ATM Transactions. IEEE Transactions on Information Security, 15(5), 250-268.

[14]. Singh, K., & Kumar, A. (2019). A Review on ATM Security Enhancements Using RFID and Biometrics. International Journal of Security and Applications, 12(9), 75-90.

[15]. Srivastava, P., &Tiwari, J. (2018). Secure ATM Transactions Using Biometric Authentication Systems. Journal of Information Technology Security, 6(4), 195-208.

[16]. Wang, T., & Lee, H. (2020). Secure ATM Transactions Using Fingerprint and Iris Recognition System. Journal of Artificial Intelligence and Security, 10(3), 305-322.

[17]. Zhang, X., & Hu, W. (2021). AI and Machine Learning for ATM Fraud Detection. Journal of Cybercrime Prevention, 9(2), 220-240.

[18]. Alzahrani, S., & Ahmed, M. (2020). A Novel Biometric-Based ATM Security System Using RFID and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, February 2025

Face Recognition. Proceedings of the International Conference on Advanced Computing, 22(4), 145-160.

[19]. Bose, P., &Sen, R. (2019). Fraud Detection in ATM Transactions Using RFID and Biometric Methods. Proceedings of IEEE Cyber Security Conference, 25(2), 98-112.

[20]. Chandrasekaran, R., &Rao, P. (2018). Design and Implementation of a Secure ATM System Using Multi-Factor Authentication. ACM Conference on Security Innovations, 17(3), 55-70.

[21]. Han, L., & Chang, Y. (2021). RFID and Palm Vein Biometrics for ATM Security: A Comparative Study. Proceedings of the International Conference on Computer Security, 14(1), 205-220.

[22]. Kapoor, V., &Mehra, S. (2020). Face and Fingerprint Recognition-Based ATM Security System. IEEE International Conference on Advanced Security Systems, 19(6), 110-125.

[23]. Khan, A., & Prasad, R. (2021). Machine Learning Algorithms for ATM Fraud Prevention Using Biometrics and RFID. Proceedings of the 15th International Cyber Security Symposium, 20(8), 140-160.

[24]. Malik, R., &Chouhan, N. (2019). An Improved Multi-Biometric ATM Security System Using RFID and Iris Recognition. Proceedings of IEEE SecureTech Conference, 13(5), 78-92.

[25]. Nakamura, S., & Yoshida, H. (2021). Application of Blockchain in Securing Biometric ATM Transactions. Proceedings of the Global Financial Security Summit, 27(2), 310-328.

[26]. Patel, V., & Raj, P. (2020). A Hybrid Approach for ATM Security Using RFID and Behavioral Biometrics. Proceedings of the International Conference on Smart Banking Security, 12(4), 200-215.

[27]. Cybersecurity Research Institute. (2021). Advances in ATM Security: The Role of Biometrics and RFID. Retrieved from www.cybersecurity-research.com

[28]. IBM Security. (2019). How RFID Technology is Enhancing ATM Security. Retrieved from www.ibmsecurity.com

[29]. Kaspersky Lab. (2020). Biometric Authentication in ATMs: Security Challenges and Solutions. Retrieved from www.kaspersky.com

[30]. McAfee Security Report. (2021). Fraud Prevention in ATMs Using RFID and Biometrics. Retrieved from www.mcafee.com

[31]. National Institute of Standards and Technology (NIST). (2020). Guidelines for Multi-Factor Authentication in Financial Transactions. Retrieved from www.nist.gov

[32]. Norton Cybersecurity. (2021). How Face Recognition is Making ATMs More Secure. Retrieved from www.norton.com

[33]. ResearchGate. (2020). ATM Security Enhancement Using Multi-Modal Biometrics. Retrieved from www.researchgate.net

[34]. SANS Institute. (2019). A Review of Biometric and RFID-Based Security Solutions for ATMs. Retrieved from www.sans.org

[35]. World Bank. (2020). Financial Inclusion and ATM Security: Challenges and Opportunities. Retrieved from www.worldbank.org