IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 7, June 2025

Impact Factor: 7.67

# Advance ATM Security System

**Mrs. A. A. Deshpande, Omprakash Patane, Mahesh Pawar, Sandeep Patil**

Department of Electronics and Telecommunication Engineering

Smt. Kashibai Navale College of Engineering, Pune, India.

**Abstract:** *In today's rapidly evolving world, ensuring the safety and security of people and property has become a top priority. This project introduces an Advanced Security System that leverages the power of modern electronics, smart sensors, and real-time communication technologies to provide a reliable and efficient security solution. The system integrates a combination of motion sensors, biometric verification (such as fingerprint or facial recognition), RFID access, and IoT-based monitoring to detect and prevent unauthorized entry*

**Keywords***:* Advanced Security System, IoT Security, Biometric Access, RFID, Motion Detection, GSM Alerts, Real-time Monitoring, Smart Lock, Surveillance, Embedded System, Intruder Alert, Home Automation, Arduino, ESP32, PIR Sensor.

## I. INTRODUCTION

In the current era of technological advancement, ensuring the safety and security of people, assets, and properties has become a critical necessity. With the increasing number of security breaches, thefts, and unauthorized intrusions, traditional security systems are often inadequate or too slow to respond in real-time. To address these challenges, this project proposes the development of an Advanced Security System that combines automation, real-time monitoring, and smart alert mechanisms to enhance the overall safety of a location.

The proposed system is built using modern components such as microcontrollers (Arduino/ESP32/Raspberry Pi), sensors (PIR, IR), biometric modules (fingerprint or face recognition), RFID cards, and GSM modules for communication. When an unauthorized person attempts to access a restricted area, the system detects the intrusion using motion or biometric sensors and triggers an alarm while sending an instant SMS or notification to the user or concerned authority. This ensures a quick response time and allows remote monitoring and control, making the system highly reliable and effective.

In addition to intrusion detection, the system supports smart locking mechanisms, camera integration for surveillance, and can be connected to a mobile app or cloud server using IoT (Internet of Things) technology. This enables users to remotely monitor their premises, receive live updates, and take appropriate actions from anywhere in the world.

The entire setup is designed to be modular, scalable, and cost-effective, making it suitable for a wide range of applications such as homes, offices, banks, schools, and other critical infrastructures. It also supports future upgrades like voice control, AI-based threat recognition, and machine learning-based behavior analysis. In conclusion, this Advanced Security System offers a smart, automated, and responsive approach to modern-day security needs, effectively blending technology with practicality to ensure maximum safety and convenience.

Objectives:

- To design a smart and reliable security system that ensures safety against unauthorized access and intrusion.
- The system aims to integrate modern technologies such as biometric authentication (fingerprint or face recognition), RFID access control, motion detection sensors, and GSM or IoT modules for real-time alerts and remote monitoring.
- Another important objective is to provide remote access and monitoring capabilities through internet or mobile communication, allowing users to manage their security system from anywhere in the world. The system is also designed to be modular, scalable, and cost-effective, ensuring that future upgrades like camera integration, AI-based threat detection, or cloud storage can be easily added.

DOI: 10.48175/568

## II. LITERATURE REVIEW

Yang, M., Xu, L., & Wang, Z. (2021)) –Biometric-Based Authentication for Internet of Things Access Control Systems
In their review on biometric-based authentication for IoT access control systems, Yang et al. emphasize how biometric modalities like fingerprint, face, iris, and voice recognition can provide highly secure and user-friendly access control compared to traditional password systems. They discuss challenges like data privacy, spoofing attacks, and computational constraints in IoT devices and propose adaptive authentication mechanisms to overcome these. Their study is pivotal in understanding how biometrics improve accuracy and security in smart environments.
Key takeaway: Biometric systems increase security and ease of use but need to address privacy and spoofing vulnerabilities.

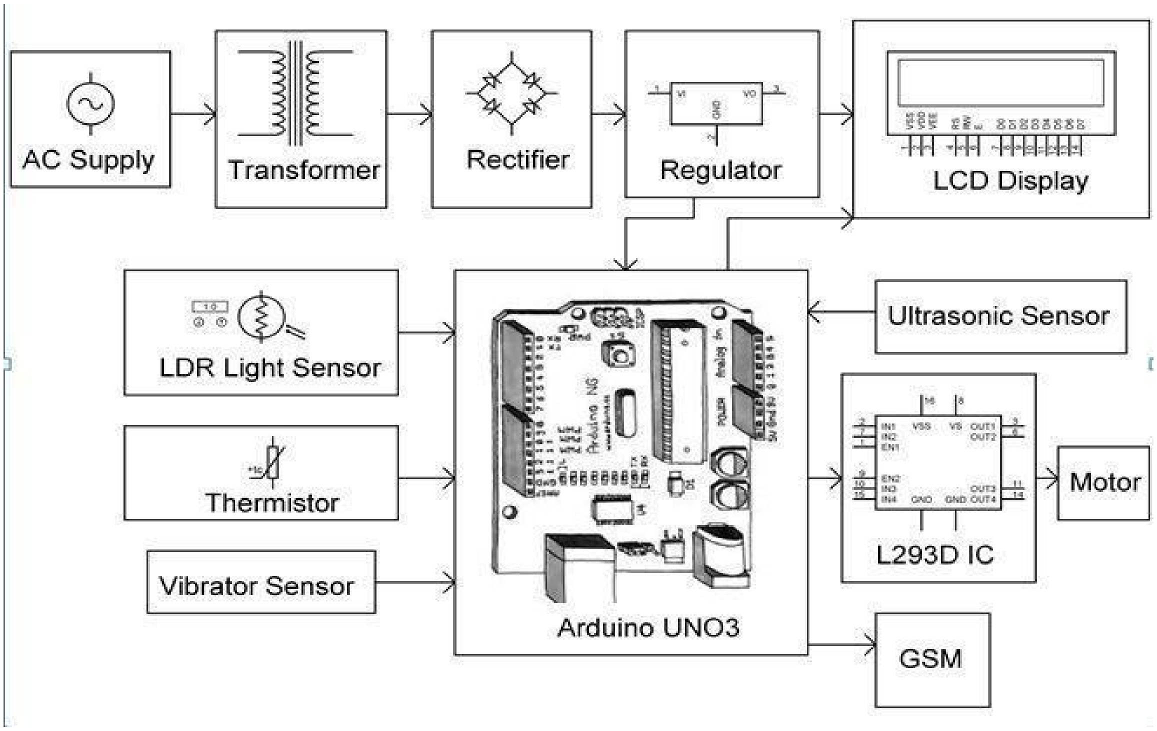
Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2024) – security challenges faced by RFID in IoT ecosystems
This paper reviews the security challenges faced by RFID in IoT ecosystems, particularly issues related to cloning, eavesdropping, and unauthorized tracking. The authors propose enhanced cryptographic protocols and lightweight encryption techniques that can be implemented in resource-constrained RFID tags. Their findings highlight the critical need to balance security with power and cost efficiency in real-world deployments.
Key takeaway: Effective cryptographic methods must secure RFID systems while preserving their low-cost and low-power characteristics.

Mansoor, A., Ghayyur, S. A., & Munir, A. (2019)– A robust authentication protocol based on symmetric cryptography for RFID- based IoT devices.
Mansoor and colleagues propose a robust authentication protocol based on symmetric cryptography for RFID-based IoT devices. Their scheme provides mutual authentication, data confidentiality, and resistance to common attacks such as replay and man-in- the-middle. Integrating GSM modules allows the system to send real-time SMS alerts, making it practical for remote security monitoring. This paper is useful in designing secure communication between the security system and the user. Key takeaway: Symmetric cryptography can secure IoT devices while enabling efficient GSM- based alerting.

Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2016) – authentication protocols tailored for the IoT environment
The authors present a comprehensive survey of existing authentication protocols tailored for the IoT environment. They classify protocols based on their security features, computational overhead, and suitability for different IoT applications, including home automation and security systems. This work highlights the trade-offs between security, latency, and power consumption, guiding developers on selecting appropriate protocols for advanced security systems.
Key takeaway: Selecting the right authentication protocol is critical to balance security and system performance.

El Gaabouri, A., El Azhari, J., & Ouahmane, H. (2023)– authentication and threat challenges in RFID-based NFC applications
Their systematic review on authentication and threat challenges in RFID-based NFC applications focuses on emerging threats such as relay attacks, tag cloning, and data interception. They discuss the importance of lightweight cryptographic algorithms that can be integrated into NFC/RFID tags without compromising performance. The paper also reviews existing authentication schemes and highlights gaps where new research is needed, particularly in scalable, energy-efficient security designs. Key takeaway: Continuous research is necessary to develop secure and scalable authentication solutions for RFID and NFC in IoT security.

## III. BLOCK DIAGRAM



This diagram illustrates a microcontroller-based monitoring and control system using the Arduino UNO3 as the central processing unit. The system begins with an AC power supply, which is stepped down by a transformer to a lower AC voltage. This voltage is then converted to DC using a rectifier and further regulated to a stable output by a voltage regulator to ensure safe and consistent power delivery to the components, including the Arduino, sensors, and LCD display. The LCD is used to display system information or sensor data in real-time.

The Arduino UNO3 receives inputs from multiple sensors to monitor environmental conditions. An LDR (Light Dependent Resistor) sensor detects ambient light levels, a thermistor measures temperature, and a vibration sensor identifies mechanical vibrations or shocks, possibly indicating movement or impact. An ultrasonic sensor is used to measure distances to objects, typically for obstacle detection or proximity sensing. These sensors feed data into the Arduino, which processes the information based on predefined logic.

Based on the sensor inputs, the Arduino controls various output components. It uses an L293D motor driver IC to operate a motor, which can perform tasks such as rotating or moving parts of the system. Additionally, the system includes a GSM module that allows the Arduino to send SMS alerts or communicate with a remote user via the mobile network, enhancing its utility in security or remote monitoring applications. Overall, this integrated system is designed for automation and monitoring purposes, suitable for applications like home automation, environmental sensing, robotics, or alert systems.

## IV. CONCLUSION

In conclusion, the Advanced ATM System is a forward-looking innovation that aligns with global trends in digital banking, cyber security, and customer-centric automation. It holds immense potential for widespread deployment, especially in high- risk or high-volume environments. With continued research and development, such systems can evolve into fully autonomous, AI-powered banking terminals of the future. The implementation of an Advanced ATM System marks a significant improvement in the security, reliability, and efficiency of modern banking services. By utilizing image processing, biometric feature extraction, and AI-based classification, the system minimizes the chances of fraud, enhances user authentication, and ensures that only authorized individuals can access sensitive financial services

Unlike traditional ATM systems that rely on PINs or magnetic cards which can be stolen or duplicated this smart solution leverages real-time face recognition or fingerprint verification to verify users with high accuracy. This not only improves user experience by making transactions faster and more seamless, but also adds a powerful layer of protection against identity theft and cybercrime

## REFERENCES

[1] Ajaykumar M (2013). “Anti-Theft ATM Machine Using Vibration Detection Sensor” International Journal of Advanced Research in Computer Science and Software Engineering, pp: 23-28

[2] Automobile Anti-theft System Based on GSM and GPS Module, Published in Intelligent Networks and Intelligent Systems (ICINIS), 2012 Fifth International Conference, Authors: Hu Jian-ming, Tianjin Univ. of Technol. & Educ, Tianjin, China, Li Jie ; Li Guang-Hui

[3] Refaie, M.N. Compute. Eng. Dept., Kuwait Univ, Kaldiya, Kuwait Selman, A. A.; Ahmad, I. 2012 “Hybrid parallel approach based on wavelet transformation and principle component analysis for solving face recognition problem” IEEE conference on Volume: 2007

[4] R. Gross, J. Shi, and J. Cohn. Quo Vadis Face Recognition? Third Workshop on Empirical Evaluation Methods in Computer Vision, December, 2011.

[5] Das, S. & Debbarma, J.(2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in India eBanking system. International Journal of Information and Communication Technology Research vol 1 no 5 p 197-203.

[6] Devinaga, R. (2010). ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450-2275 issue 21.

[7] Yadav, R. & Bhardwaj, S. (2019). Smart ATM security system using IoT. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(6), 650–654.

[8] Singh, A., & Arora, A. (2016). Enhanced ATM Security System Using Biometric and GSM Technology. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5(4), 1203–1206.

DOI: 10.48175/568