International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802171

An Intelligent IoT-Driven ATM Security System with Invisible Keypad and User Detection

Revathy G, Shaalini J, Stenee Maria G, M. Maheswari

Department of Electronics and Communication Engineering, Sethu Institute of Technology, Virudhunagar, India

Guide, AP, Department of Electronics and Communication Engineering, Sethu Institute of Technology, Virudhunagar, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: The project titled "An Intelligent IoT-Driven ATM Security System with Invisible Keypad and User Detection" presents a smart and secure ATM system aimed at enhancing user privacy and preventing unauthorized access during PIN entry. It integrates hardware components such as Arduino Uno, ultrasonic and IR sensors, RFID module, and buzzer with ATM software developed using Python and a MySQL database. The system activates only when a valid user is detected, and it dynamically hides the keypad if any suspicious presence is identified. Additionally, the keypad layout is shuffled each time to prevent pattern tracking. The system consists of two main modules: the Account Management Module and the ATM Module. The Account Management Module enables administrators to create and manage user accounts with features like CRUD operations, secure storage of account details, and automatic PIN generation. User credentials are stored in the database and shared securely via email, ensuring proper record maintenance and secure communication. The ATM Module handles user transactions such as deposit, withdrawal, balance enquiry, mini statement, and PIN change with OTP verification. During PIN entry, sensors continuously monitor for unauthorized presence, making the keypad invisible if any threat is detected. Overall, the system enhances ATM security, ensures user privacy, and provides a reliable solution to prevent fraud and unauthorized observation.

KEYWORDS: ATM Security, Invisible Keypad, RFID Authentication, Ultrasonic Sensor, PIN Protection, Shoulder Surfing Prevention

I. INTRODUCTION

In today's digital era, Automated Teller Machines (ATMs) play a vital role in providing convenient and 24/7 banking services to customers. ATMs allow users to perform essential banking transactions such as cash withdrawal, deposit, balance enquiry, fund transfer, and PIN change without visiting bank branches. Despite their convenience, ATM systems are increasingly vulnerable to security threats such as shoulder surfing, PIN theft, card skimming, hidden cameras, and unauthorized access. Among these threats, PIN exposure during entry is one of the most common and serious security concerns. Criminals often observe users while they enter their PIN, compromising personal and financial information. To address these challenges, the project titled **"An Intelligent IoT- Driven ATM SecuritySystem with Invisible Keypad and User Detection"** proposes a smart, sensor-based security system that enhances user privacy during ATM transactions. The system integrates IoT technology with hardware components such as Arduino Uno, Ultrasonic Sensor, IR Sensor, RFID module, and Buzzer, along with ATM software developed using Python and MySQL. The primary objective of this project is to create a secure ATM environment where the keypad dynamically becomes invisible whenever suspicious activity is detected, thereby preventing unauthorized observation during PIN entry.

II. LITERATURE SURVEY

Shoulder Surfing Attacks in ATM PIN Entry(2024)

Kumar and Singh (2024) in *IEEE Transactions on Information Forensics and Security* identified shoulder surfing as a significant threat to user privacy in authentication systems. The study explains that attackers can easily observe PIN entry or passwords in public places without the user's knowledge. This type of attack is difficult to detect and prevent using traditional security methods. The authors highlight that such attacks can lead to serious consequences like identity theft and financial fraud. To address this issue, the research proposes solutions such as dynamic keypads, randomized input layouts, and visual obfuscation techniques. These methods reduce the risk of attackers predicting or capturing

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802171

sensitive information. The study also emphasizes the importance of balancing security with usability. Overall, it suggests that adaptive and user- friendly security mechanisms are essential for modern systems.

IoT Sensors for Real-Time Monitoring and Security (2023)
Chen and Zhao (2023) in the *International Journal of IoT Applications* discussed the importance of IoT sensors in modern security systems. The study highlights how sensors such as ultrasonic, IR, and motion detectors can continuously monitor user activity and surroundings. These sensors help in detecting unusual behavior or unauthorized presence in real time. The research explains that real-time monitoring enables quick system responses, such as triggering alerts or activating security measures. It also discusses the integration of sensors with microcontrollers for automated decision-making. The system improves efficiency by reducing human intervention in security monitoring. Additionally, the authors emphasize the scalability of IoT-based systems across various applications. This approach significantly enhances safety and reliability.

Python and MySQL Based Banking System (2020)
Patel and Rao (2020) in the *International Journal of Computer Applications* developed a banking system using Python and MySQL. The study focuses on creating a secure and efficient platform for managing banking operations. It explains how Python is used for application development due to its simplicity and flexibility. MySQL is utilized for structured data storage and management of user information. The system supports essential functions such as account creation, transactions, and balance updates. The authors also emphasize secure query execution to prevent data breaches. The research highlights the importance of maintaining data integrity and consistency. Overall, it provides a strong foundation for developing secure banking applications.

ATM Security with Deep Learning for Movement Detection(2025)
Patel and Bharatbhai (2025) proposed an advanced ATM security system using deep learning techniques for movement detection. The study focuses on identifying suspicious human activities around ATM machines by analyzing real-time video or sensor data. By applying deep learning algorithms, the system can accurately distinguish between normal user behavior and unusual movements, such as the presence of multiple people or suspicious gestures during PIN entry. This helps in preventing threats like shoulder surfing and unauthorized access. The research highlights the advantage of using intelligent models that continuously learn and improve detection accuracy over time. Additionally, the system can trigger alerts or security actions when abnormal activity is detected, ensuring immediate response. Overall, the study demonstrates how integrating deep learning with ATM security systems enhances surveillance, improves threat detection, and provides a more reliable and intelligent solution for protecting user privacy.

IP Camera ATM Surveillance (2023): Integrated ATM Monitoring System
The 2023 study on IP camera-based ATM surveillance presents an integrated monitoring system designed to enhance ATM security through continuous video surveillance. The system utilizes IP cameras to capture real-time footage of user activity around the ATM, enabling remote monitoring and recording of transactions. It focuses on detecting suspicious behaviors such as loitering, multiple person presence, and unauthorized access attempts. The captured video data can be stored in cloud or local servers for future analysis and evidence. The study also highlights the use of motion detection and alert mechanisms to notify authorities in case of abnormal activity. Compared to traditional CCTV systems, IP cameras provide higher resolution, remote accessibility, and better scalability. Overall, the integrated surveillance system improves security, supports incident investigation, and ensures safer ATM environments.

Multi Factor ATM System (2024): Biometric and OTP Combination
The 2024 study on a multi-factor ATM system proposes a secure authentication approach by combining biometric verification with OTP (One-Time Password) validation. The system requires users to first authenticate using biometric data such as fingerprint or facial recognition, followed by an OTP sent to their registered mobile number or email. This dual- layer authentication significantly reduces the risk of unauthorized access, even if one credential is compromised. The study highlights that biometric identification ensures user uniqueness, while OTP provides a dynamic and time-sensitive security layer. It also discusses how this approach effectively prevents common ATM frauds such as PIN theft, card cloning, and identity misuse. Additionally, the system is designed to be user-friendly while maintaining high security standards. Overall, the integration of biometric and OTP authentication enhances ATM security, improves user trust, and provides a robust solution for modern banking systems.

Automated Teller Machine Security and Robbery Prevention Based on Human Behaviour Analysis (2023)
This study focuses on enhancing ATM security by analyzing human behavior to detect potential threats and prevent robbery attempts. The system uses cameras and sensors to monitor user actions such as body movement, gestures, and

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

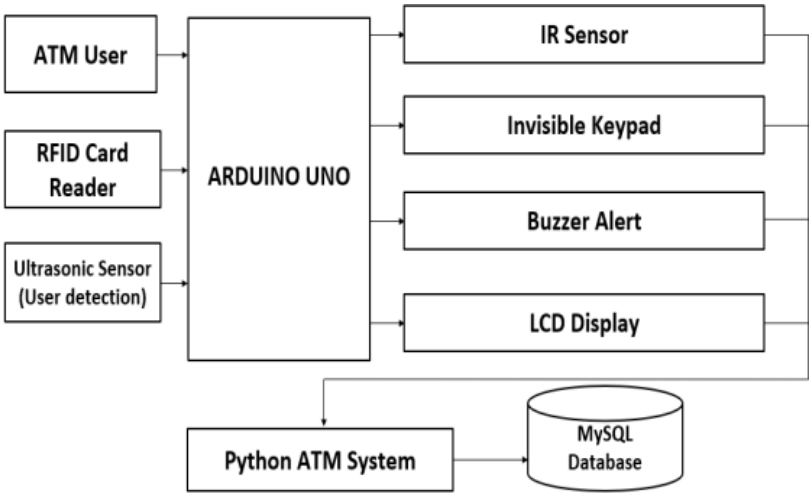
DOI:10.15662/IJEETR.2026.0802171

unusual activities around the ATM. By applying behavior analysis techniques, it can differentiate between normal transactions and suspicious actions like loitering, forced interactions, or aggressive movements. The research highlights that early detection of abnormal behavior allows the system to trigger alerts, activate alarms, or notify authorities in real time. It also discusses the use of intelligent algorithms to improve detection accuracy and reduce false alarms. Compared to traditional security systems, behavior-based analysis provides a proactive approach to threat prevention. Overall, the study demonstrates that integrating human behavior analysis into ATM systems can significantly improve security, prevent robberies, and ensure user safety.

III. PROPOSED SYSTEM

The proposed system, "IoT Based Invisible Keypad for ATM Privacy," is designed to provide a highly secure and privacy- focused ATM environment by preventing unauthorized observation during PIN entry. The system integrates both hardware and software components, including Arduino Uno as the main controller, ultrasonic sensor for user detection, IR sensor for identifying nearby unauthorized individuals, RFID module for card-based authentication, and a buzzer for alert notifications. The software part is developed using Python with a MySQL database to manage user accounts, authentication, and transaction records. Initially, the ultrasonic sensor detects whether a user is standing at an appropriate distance in front of the ATM. Only after confirming valid user presence does the system activate and prompt the user to scan their RFID-based ATM card for authentication.Once the card is verified, the system allows the user to proceed with PIN entry. During this process, the IR sensor continuously monitors the surroundings to detect the presence of any additional or suspicious person. If such activity is detected, the keypad immediately becomes invisible, thereby preventing PIN exposure and protecting user privacy. To further enhance security, the keypad layout is dynamically shuffled each time, making it difficult for attackers to track input patterns. In case of suspicious activity or unauthorized attempts, the buzzer is activated to alert the system or nearby authorities. After successful authentication, the user can access various banking services such as deposit, withdrawal, balance enquiry, mini statement, and PIN change.Additionally, the system includes advanced features like OTP verification for secure PIN updates, ensuring an extra layer of authentication. The MySQL database securely stores user details, account information, and transaction history, maintaining data integrity and reliability. The entire system works in real-time, enabling quick detection and response to potential threats. By combining IoT-based sensing technology with secure software implementation, the proposed system significantly enhances ATM security, minimizes the risk of fraud, and ensures a safe and user-friendly banking experience.In addition, the system enhances security through features such as shuffled keypad layout, RFID-based authentication, OTP verification for PIN changes, and secure database management. These combined hardware and software mechanisms enable real-time monitoring and multi-layer protection. Overall, the system reduces the risk of PIN theft and unauthorized access, providing a smarter and more secure ATM solution for modern banking environments.

IV. BLOCK DIAGRAM



Block Diagram Description

The block diagram of the IoT Based Invisible Keypad for ATM Privacy system illustrates the interaction between hardware components and software modules to ensure secure ATM operations. The Arduino Uno acts as the central

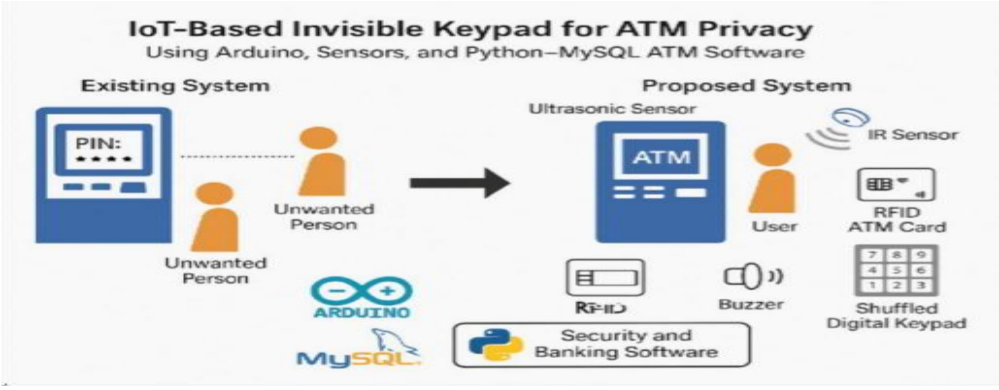
|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802171

controller, receiving inputs from the ATM user, RFID card reader, and ultrasonic sensor. The ultrasonic sensor is responsible for detecting the presence of a valid user in front of the ATM, while the RFID card reader is used for authenticating the user through card scanning. These inputs are processed by the Arduino to determine whether the system should proceed with the transaction.Based on the processed data, the Arduino controls several output components, including the IR sensor, invisible keypad, buzzer alert, and LCD display. The IR sensor continuously monitors for unauthorized individuals near the user during PIN entry, and if detected, the system activates the invisible keypad feature to hide the PIN interface. Simultaneously, the buzzer provides an alert for suspicious activity, and the LCD display shows system messages and transaction details to the user. The Arduino also communicates with the Python-based ATM system, which handles the logic for banking operations and interacts with the MySQL database to store and retrieve user and transaction information. Overall, the block diagram represents a coordinated system that combines real-time sensing, processing, and secure data management to enhance ATM security and user privacy.

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

The IoT Based Invisible Keypad for ATM Privacy system presents an innovative and practical solution to enhance security and user privacy in ATM transactions. Traditional ATM systems primarily rely on card and PIN authentication, which are vulnerable to observation attacks such as shoulder surfing and hidden camera recording. The proposed system overcomes these limitations by integrating Arduino-based sensor technology with intelligent software developed using Python and MySQL. By utilizing an ultrasonic sensor to detect user presence and an IR sensor to identify unauthorized individuals during PIN entry, the system dynamically hides the keypad whenever suspicious activity is detected. Additionally, the shuffled keypad layout, RFID-based authentication, OTP verification for PIN changes, and secure database management provide multiple layers of protection. This combination of hardware and software ensures real-time monitoring, proactive security measures, and improved transaction safety. Overall, the proposed system significantly reduces the risk of PIN theft and unauthorized access, offering a smarter, more secure, and privacy-focused ATM solution suitable for modern banking environments.

VII. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our project guide for their invaluable guidance, continuous support, and encouragement throughout the development of our project.Their expert advice, constructive feedback, and constant motivation helped us to understand the concepts clearly and successfully complete this work. We also extend our heartfelt thanks to the faculty members of the Department of Electronics and Communication Engineering for their support, knowledge sharing, and encouragement during the course of this project.This project focuses on enhancing ATM security and ensuring user privacy by integrating IoT-based hardware components such as Arduino Uno, ultrasonic sensor, IR sensor, RFID module, and buzzer with software developed using Python and MySQL. The system is designed to prevent shoulder surfing and unauthorized access by dynamically hiding the keypad during suspicious conditions, thereby improving the overall safety of ATM transactions. The successful implementation of both hardware and software modules has provided us with practical knowledge and hands-on experience in embedded systems, IoT, and database management.We would also like to thank our institution for providing the necessary infrastructure, laboratory facilities, and resources required to carry out this project successfully. We are grateful to our teammates and friends for their cooperation, valuable suggestions, and teamwork, which played an important role inovercoming challenges during the project development. Finally, we express our heartfelt gratitude to our families

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802171

ftheir continuous encouragement, moral support, and understanding, which motivated us to complete this project successfully.

REFERENCES

1. K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 2009.
2. A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A Survey of Topics and Trends," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 1–17, 2014.
3. Arduino, "Arduino Uno Rev3 Datasheet," 2023.
4. Espressif Systems, "ESP8266EX Datasheet," 2022.
5. D. Banerjee and P. Chatterjee, "Security Issues in ATM Systems," International Journal of Computer Applications, vol. 57, no. 15, 2012.
6. M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man-in-the- Middle Attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, 2016.
7. Python Software Foundation, "Python Documentation – GUI and Database Connectivity," 2023.
8. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
9. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
10. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
11. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
12. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
13. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
14. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
15. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
16. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
17. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
18. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
19. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
20. Oracle Corporation, "MySQL 8.0 Reference Manual," 2023.
21. S. Singh and N. Sharma, "Design and Implementation of Secure ATM Systems Using Embedded Systems," International Journal of Advanced Research in Computer Science, 2018.
22. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, 2015.
23. Sudha, N., Kumar, S. S., Rengarajan, A., & Rao, K. B. (2021). Scrum Based Scaling Using Agile Method to Test Software Projects Using Artificial Neural Networks for Block Chain. *Annals of the Romanian Society for Cell Biology, 25(4), 3711-3727.*
24. Sugumar, R. (2025). Designing Resilient and Scalable Cloud-Native Frameworks for Generative AI Content Production. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13268-13279.*
25. Anbazhagan, K. (2025). AI Driven Zero Trust Security Model for Enterprise Data Protection and Intelligent Infrastructure Management. *International Journal of Technology, Management and Humanities, 11(03), 101-107.*
26. Gowtham, M. S., Ramkumar, M., Jamaesha, S. S., & Vigenesh, M. (2024). Artificial self-attention rabbits battle royale multiscale network based robust and secure data transmission in mobile Ad Hoc networks. *Computers & Security, 142, 103889.*
27. Prabha, S. P., & Rengarajan, A. (2025, February). Decentralized Resource Allocation Model Using Multi-agent Reinforcement Learning for Cloud Environment. In *International Conference on Universal Threats in Expert Applications and Solutions* (pp. 71-82). Singapore: Springer Nature Singapore.