Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 15 Issue 01, 2026

RFID-Based Intelligent Access Control and Monitoring System

[1]Shrikant Sunil Joshi, [2]Rutuja Umesh Dudhane, [3]Riddhi Prasad Chavan, [4]M. R. Jadhav
[1,2,3] Department of Electronics and Telecommunication Engineering, Dr. J.J. Magdum College of Engineering, Jaysingpur, India
[4]Project Guide, Department of Electronics and Telecommunication Engineering, Dr. J.J. Magdum College of Engineering, Jaysingpur, India
Email: [1]shrikantj2504@gmail.com

Peer Review Information

Submission: 10 April 2026

Revision: 01 May 2026

Acceptance: 22 May 2026

Keywords

RFID, IoT, Embedded Systems, Access Control, Flask, SQLite, Security System, Monitoring

Abstract

This paper describes the conceptualization and deployment of a smart, RFID-driven security and personnel monitoring framework built upon Internet of Things (IoT) principles. The primary objective is to bolster organizational security through instantaneous identity verification, controlled entry management, and continuous individual tracking via RFID-enabled cards. The architecture merges physical hardware — consisting of RFID scanning units and embedded microcontrollers — with a software layer built on the Flask web framework and an SQLite relational database. Notable capabilities include detection of blacklisted individuals, multi-gate surveillance, automated alarm activation, and a centralized administrator interface for data visualization.

Introduction

Contemporary organizations are increasingly adopting intelligent technologies to streamline personnel management workflows. Conventional entry control approaches suffer from inflexibility, weak security postures, and an inability to track personnel movements in real time, culminating in operational inefficiencies. The Multipass Employee Management System was conceived to overcome these shortcomings by coupling RFID identification technology with an IoT infrastructure, thereby delivering automated, dependable, and secure access regulation.

A defining characteristic of this platform is that a single RFID credential grants an employee access to every location they are authorized to enter, with privileges determined by their organizational role. The study examines how the convergence of embedded computing and server-side software can improve entry management, live personnel tracking, and threat monitoring. It further investigates how physical hardware can be woven into web-based management platforms to enable uninterrupted oversight and centralized administration, touching on system architecture, data persistence strategies, and live data handling.

Notwithstanding its merits, the technology presents several deployment challenges. Constraints such as the restricted operational range of RFID hardware, reliance on device uptime, and vulnerabilities in data handling can undermine system reliability. Furthermore, keeping access privilege lists accurate and safeguarding stored data are non-trivial concerns. Deploying real-time tracking also introduces questions around worker privacy and responsible data governance within enterprise settings.

This investigation examines the Multipass system through a structured lens — analyzing its architectural blueprint, operational mechanics, and real-world performance — while

also appraising its strengths, known constraints, and avenues for future enhancement. The following research questions guide the inquiry:

RQ1: In what ways does the Multipass platform strengthen workforce access governance and physical security?

RQ2: Which underlying technologies — RFID, IoT, and web services — constitute the system's foundation?

RQ3: What practical difficulties and inherent limitations arise during system deployment?

RQ4: What strategies and enhancements can expand system throughput and scalability?

RQ5: What security and privacy implications stem from continuous, real-time workforce monitoring?

Methodology

The Multipass system's development methodology centers on harmonizing RFID identification, embedded computing, and web application technologies to achieve reliable access management and live monitoring. The architecture is built to accommodate numerous access points while enforcing role-specific privileges for all personnel. The build process encompasses hardware configuration, server-side development, database construction, and end-to-end system integration.

1. System Architecture

At its core, the system consists of RFID readers interfaced with a microcontroller that relays data to a Flask-powered backend server. Every employee is issued a distinct RFID token carrying a unique identifier (UID), which the SQLite database maps to the holder's profile and permitted zones. The framework accommodates multiple checkpoints and enforces zone-specific restrictions aligned with each employee's predefined role.

2. Data Capture and Processing

Data originates from RFID card interactions at individual access nodes. Every interaction produces a record comprising the UID, checkpoint identifier, event timestamp, and admission outcome. These records are relayed to the backend, where identity and authorization checks are performed before the data is written to the database for audit and operational review.

3. Authorization Control Framework

Authorization is enforced through a privilege matrix tied to each employee's organizational role. Upon card presentation, the system validates whether the cardholder holds the requisite clearance for the target checkpoint. A validated credential triggers an access grant; an invalid or unauthorized credential produces an alert and denial. This mechanism ensures restricted zones remain accessible only to cleared personnel.

4. Deployment Details

Deployment required writing firmware for the embedded controller to manage RFID reader communication and server data relay. The Flask backend handles incoming requests, executes validation logic, and manages database interactions. A browser-accessible management console enables administrators to observe live activity, maintain user records, and review event logs.

5. Audit Trail and Logging

The system captures granular records of all ingress and egress events, documenting both successful authentications and rejected attempts. This audit trail supports workforce movement analysis and retrospective investigation of security breaches. The admin console surfaces both real-time feeds and historical trend visualizations to inform operational decisions.

6. Constraints and Known *Challenges*

Deployment hurdles include hardware fragility, the limited scan range of RFID technology, and latency in network-dependent real-time data flows. Ongoing surveillance of employee activity also raises data protection and privacy considerations. Addressing these issues demands careful system tuning and a proactive maintenance strategy.

Results And Discussion

RQ1 — Access Control and Security Enhancement: The platform materially improves access governance by empowering employees to use a solitary credential across all authorized zones, with privileges dynamically governed by role assignments. Every entry request is resolved in real time, guaranteeing that restricted areas remain sealed to unauthorized individuals. Any breach attempt is logged instantly, elevating overall security posture. Automating the authentication process also eliminates human-induced errors and delivers uniform policy enforcement at every access node.

RQ2 — Underlying Technologies: The solution draws on a synergy of RFID readers for credential scanning, microcontrollers for hardware-software mediation, Flask for server-side logic, and SQLite for storing employee profiles, authorization data, and event records. Together these components yield a cohesive platform capable of live monitoring and centralized operational control.

RQ3 — Challenges and Constraints: The system contends with hardware-imposed limitations — notably the narrow effective range

of RFID readers and dependency on device reliability — alongside network latency that can disrupt real-time communication. Managing access permissions for large employee populations adds administrative complexity, while the sensitivity of stored personnel data necessitates robust security safeguards to prevent unauthorized database access.

RQ4 — Performance and Scalability Improvements: Future iterations could adopt wireless-capable controllers such as the ESP32 to eliminate wired dependencies and extend deployment flexibility. Migrating to cloud-hosted data stores would enhance capacity, remote operability, and resilience. Incorporating cryptographic protections and optimizing backend throughput would reduce response latency, while layering in biometric verification would reinforce authentication strength.

RQ5 — Security and Privacy Implications: Continuous workforce tracking inherently raises concerns about employee privacy and the potential for data misuse. Exposure of movement logs or personal records could breach confidentiality. Mitigating these risks requires encrypted storage, strictly controlled admin access, and transparent organizational policies that clearly define the boundaries and ethical scope of monitoring activities.

Key Findings Summary: The Multipass system demonstrates measurable gains in access control effectiveness, physical security, and operational productivity. Its tight hardware-software integration enables automated decision-making and live situational awareness. While hardware constraints and data protection challenges persist, targeted technological upgrades can address these gaps. The project validates the viability of IoT-driven solutions for enterprise-grade workforce management.

Conclusion

The Multipass Employee Management System constitutes a robust and dependable mechanism for contemporary access regulation and workforce oversight. By fusing RFID identification with embedded computing and web-based administration, it delivers automated, real-time control over personnel movement across an organization's physical footprint. Role-derived authorization confines zone access to cleared individuals, meaningfully elevating security and streamlining operations.

The platform validates the practical utility of IoT-enabled solutions in addressing tangible enterprise security challenges. Capabilities such as live monitoring, unified control, and automated event logging reduce dependence on manual oversight and support faster, evidence-based decision-making. The adoption of Flask and SQLite ensures efficient data flow and reliable persistence.

Residual challenges — hardware reliability constraints, RFID range limitations, and data security exposures — remain areas requiring deliberate attention. With systematic enhancements, the platform is well-positioned to scale for larger deployments and more demanding operational environments. In its current form, it establishes a solid technical foundation from which more sophisticated, intelligent access
control systems can evolve.

Future Work

Several advancement paths can meaningfully extend the Multipass system's capabilities. Replacing current microcontrollers with wireless-native alternatives — such as the ESP32 family — would eliminate wired infrastructure dependencies, enabling flexible deployment in large or geographically distributed facilities.

Transitioning from on-premise SQLite storage to cloud-based database services would provide elastic scaling, geographic redundancy, and remote administration. Complementing this with end-to-end data encryption, hardened authentication flows, and granular role-based admin permissions would substantially strengthen the system's security posture.

Multi-factor authentication — specifically biometric modalities such as fingerprint scanning or facial recognition — layered on top of RFID credentials would dramatically reduce impersonation risks. A dedicated mobile application for administrators could further streamline remote surveillance, push notifications, and system configuration.

Integrating machine learning models to analyze movement patterns and flag behavioral anomalies would transform the system from reactive to predictive. AI-driven resource optimization could additionally improve facility utilization efficiency. Collectively, these enhancements would evolve the Multipass platform into an intelligent, adaptive enterprise security solution capable of meeting the demands of modern organizations.

Acknowledgment

The author extends sincere appreciation to the faculty of the Department of Electronics and Telecommunication Engineering for their expert mentorship and unwavering encouragement. Gratitude is also due to the institution for furnishing the resources necessary to undertake this work, and to peers and colleagues whose

collaborative discussions enriched the development process. The author's family deserves special recognition for their consistent moral support throughout the project.

References

K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 3rd ed. Wiley, 2010.

D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, Newnes, 2012.

S. A. Ahson and M. Ilyas, *RFID Handbook: Applications, Technology, Security, and Privacy*, CRC Press, 2017.

K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 2009.

L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, 2010.

J. Gubbi et al., "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, 2013.

A. Banks and R. Gupta, "MQTT Version 3.1.1," OASIS, 2014.

H. Ning and H. Liu, "Cyber-Physical-Social-Based Security Architecture," 2012.

S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," 2015.

P. S. Pandey and A. K. Singh, "RFID-based attendance system," 2014.

M. Hossain and G. Muhammad, "Cloud-assisted IoT platform," *IEEE IoT Journal*, 2016.

A. Zanella et al., "IoT for smart cities," *IEEE IoT Journal*, 2014.

S. Madakam et al., "IoT: A literature review," 2015.

R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, 2006.

N. K. Verma and R. Gupta, "RFID-based security system," 2015.

M. Burhan et al., "RFID-based smart attendance system," 2018.

S. Kumar and P. Tiwari, "IoT-based smart security system," 2019.

Flask Documentation, "Flask Web Framework." https://flask.palletsprojects.com

SQLite Documentation, "SQLite Database Engine." https://www.sqlite.org

R. Fielding, "Architectural Styles and REST," 2000.

D. Comer, *Internetworking with TCP/IP*, 2015.

A. Silberschatz et al., *Database System Concepts*, 2019.

T. Erl, *Cloud Computing Concepts*, 2013.

A. Tanenbaum, *Computer Networks*, 2011.

J. Kurose and K. Ross, *Computer Networking*, 2017.

A. S. Malik et al., "Security issues in IoT," *IEEE Access*, 2018.

M. Abomhara and G. M. Køien, "Security and privacy in IoT," 2014.

B. Schneier, *Applied Cryptography*, 2015.

P. Mell and T. Grance, "NIST Cloud Definition," 2011.

Y. Lu and L. Da Xu, "IoT cybersecurity research," *IEEE IoT Journal*, 2019.

Author Biography

Shrikant Joshi is an undergraduate student in Electronics and Telecommunication Engineering with a focused interest in Embedded Systems, the Internet of Things, and Artificial Intelligence. He has accumulated hands-on experience across embedded system prototyping, mobile application development, and real-time system implementation. His project portfolio includes an autonomous fire-suppression robot and RFID-enabled intelligent systems, and he has served as a technical mentor for students in applied technology programs.