

Microcontroller-Based Security Systems for Restricted Buildings: A Review of Existing Approaches and Research Gaps.

Maduka Nosike C¹, Kamal H Sarkinpawa², Yahaya Yusuf³, Francis I Okoye⁴

Department of Physics, Federal University Gusau, Nigeria

Corresponding Author's Email: kspawa4866@gmail.com

Received on: August, 2026

Revised and Accepted on: September 2026

Published on: October, 2026

ABSTRACT

The protection of restricted buildings is important because unauthorized access, intrusion, theft, and other security threats can compromise property, information, and human safety. Traditional security approaches often depend on physical guards or single authentication mechanisms, which may provide limited coverage and may not support rapid detection and notification of security incidents. This paper reviews recent microcontroller-based and Internet of Things (IoT)-enabled security systems, with emphasis on access control, intrusion detection, vehicle identification, monitoring, communication, and simulation. A systematic search was carried out across major academic databases and indexing platforms, including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar for studies published between 2016 to 2026 to identify relevant studies and ensure broad coverage of the existing literature. The search initially identified 145 publications. After title screening, 43 studies were retained for further assessment, and 17 studies were selected for detailed analysis following abstract and full-text screening. The selected studies were compared according to their major security functions, technologies, limitations, cost and research gaps. The review shows that Radio frequency identification (RFID), biometric authentication, sensors, License Plate Recognition (LPR), computer vision, IoT, cloud and fog computing have been applied to address different security requirements. However, the reviewed systems generally concentrate on specific security functions rather than integrating access control, intrusion detection, vehicle identification, monitoring, and notification within a single platform. The review therefore identifies an opportunity for an integrated microcontroller-based security system for restricted buildings and provides a basis for its proposed design and simulation.

Keywords: Microcontroller, access control, building security, intrusion detection, restricted buildings, Internet of Things, License Plate Recognition, simulation.

1.0 INTRODUCTION

Security is an important requirement for buildings where access must be controlled and activities need to be monitored. Restricted buildings require stronger protection because unauthorized access can result in the loss of property, sensitive information, or human safety. The increasing integration of Internet of Things (IoT) devices and automated building systems has also increased the need for effective security mechanisms within connected environments (Bashir *et al.*, 2022; Gravetoet *al.*, 2022; Vardakis *et al.*, 2024). Traditional security methods, such as physical guards, mechanical locks, and basic alarm systems, are still commonly used in many environments. However, these methods may not provide continuous monitoring, automatic identification, or rapid notification when a security incident occurs (Ahangeret *al.*, 2020; Medhat *et al.*, 2020).

The development of microcontrollers has created opportunities for the design of compact and relatively low-cost electronic security systems. Microcontrollers can receive information from sensors, process the information, and control devices such as alarms, electronic locks, cameras, and communication modules

(Arjun *et al.*, 2023). The integration of microcontrollers with Internet of Things (IoT) technologies has further improved the ability of security systems to monitor events and communicate information remotely (Bashir *et al.*, 2022; Medhat *et al.*, 2020). Because many IoT and embedded devices operate with limited processing and memory resources, security mechanisms must also consider computational efficiency (Kia *et al.*, 2026; Murthy *et al.*, 2024).

Recent studies have examined different approaches to building security. RFID has been used to identify authorized users, while biometric information has been applied to strengthen authentication (Huang *et al.*, 2022; Pal & Jadidi, 2021). Other studies have used Internet-connected sensors, cameras, machine learning, fog computing, and smart-building architectures to improve monitoring and response (Martín Toralet *al.*, 2023; Medhat *et al.*, 2020; Murthy *et al.*, 2024; Pilottiet *al.*, 2026). License Plate Recognition (LPR) has also been investigated as a means of identifying vehicles entering controlled areas. Recent research has demonstrated an automated vehicle access-control system based on deep-learning LPR, indicating the potential of vehicle



identification as part of an integrated security system (Advait *et al.*, 2026).

Although security technologies have improved, many existing systems still focus on a single security function. For example, an RFID system can provide user authentication but may not detect intrusion around a building, while a surveillance system may detect suspicious activity without controlling physical access. IoT-based systems can also face vulnerabilities involving unauthorized access, denial-of-service attacks, firmware weaknesses, and other cyber threats (Bhardwaj *et al.*, 2024). Some advanced systems require substantial computing and communication resources, which can increase system complexity and create challenges for resource-constrained devices (Kia *et al.*, 2026; Murthy *et al.*, 2024). Therefore, combining complementary security functions within an appropriate architecture remains an important consideration for smart and restricted-building security.

There is therefore a need to examine existing approaches and identify their strengths and limitations before developing an improved security system. Recent research has demonstrated the application of microcontrollers, IoT, RFID, biometric authentication, intrusion detection, machine learning, smart-building architectures, and automated vehicle access control to different security problems (Advait *et al.*, 2026; Arjun *et al.*, 2023; Huang *et al.*, 2022; Martín Toralet *et al.*, 2023; Medhat *et al.*, 2020; Ovioisa&Güney, 2026). However, the integration of access control, intrusion detection, vehicle identification, monitoring, and notification within a single system specifically designed for restricted buildings remains an important area for investigation. This paper reviews selected studies related to microcontroller-based security, access control, intrusion detection, smart buildings, vehicle identification, and simulation. The review focuses on the technologies used, their security functions,

limitations, and the gaps that remain. The findings provide a basis for the proposed design and simulation of a microcontroller-based security system for restricted buildings.

2.0 METHODOLOGY

2.1 Literature Search

A literature search was conducted to identify published studies related to microcontroller-based security systems, access control, restricted areas, building security, intrusion detection, vehicle identification, premises security, facility security, IoT, and simulation. To ensure a comprehensive literature search, a structured search strategy was conducted targeting major academic repositories and indexing platforms, including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar as a comprehensive aggregator. The search targeted peer-reviewed journal articles, conference proceedings, and technical reports. The search was limited to publications dated from 2016 to 2026.

The main search query was:
("microcontroller" OR "ESP32" OR "STM32") AND ("access control" OR "restricted area" OR "facility security" OR "premises security") AND ("building security") AND simulation

Additional relevant terms were considered when examining related studies, including RFID, biometric authentication, intrusion detection, License Plate Recognition, IoT security, smart buildings, cloud computing, fog computing, and surveillance.

The initial search produced 145 publications. The retrieved publications were subsequently screened according to their relevance to the objectives of the review.

The database search parameters, keywords, and applied filters are systematically structured and summarized in Table 1.

Table 1: Method of search

Platform	Search query	Used filter
Google Scholar IEEE Xplore ScienceDirect SpringerLink	("microcontroller" OR "ESP32" OR "STM32") AND ("access control" OR "restricted area" OR "facility security" OR "premises security") AND ("building security") AND simulation	2016-2026

2.2 Inclusion and Exclusion Criteria

Studies were considered for inclusion when they were published between 2016 and 2026 and addressed one or more aspects relevant to the review, including microcontroller-based security, access control, intrusion detection, building security, premises security, facility

security, vehicle identification, IoT-enabled security, surveillance, or related security applications.

Studies were excluded when their subject matter was not sufficiently related to the objectives of the review or when they did not provide information useful for assessing security functions, technologies, cost,

limitations, or research gaps. Publications that did not provide sufficient information for assessment were also excluded.

2.3 Study Selection Process

The study selection process was conducted in stages. First, the titles of the 145 retrieved publications were examined. Publications that were clearly unrelated to microcontroller-based security, building security, access control, premises security, facility security, intrusion detection, vehicle identification, or related applications

were removed. Following title screening, 43 publications were retained for further assessment.

The abstracts and available full texts of the remaining publications were then examined. Particular attention was given to studies that described an implemented, designed, or simulated security system and provided information about its security functions, technologies, limitations, cost and possible research gaps. Following this assessment, 17 studies were selected for detailed analysis. The multi-stage study selection and screening process is detailed in Table 2.

Table 2: Literature selection process

Selection stage	Number of studies
Initial search results	145
Studies retained after title screening	43
Studies selected after abstract and full-text assessment	17

2.4 Selection flow diagram

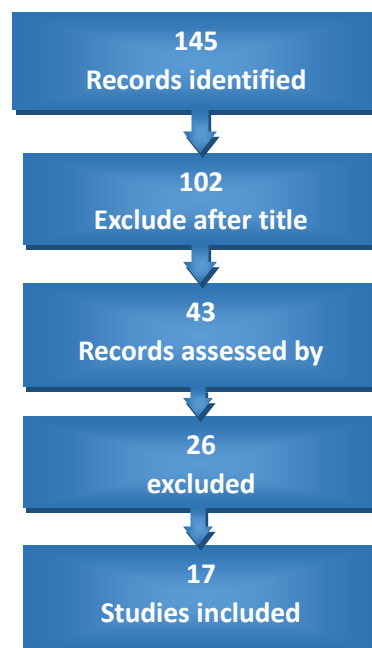


Figure 2.4: Selection flow diagram

2.5 Data Extraction and Analysis

Information from the 17 selected studies was extracted and organized according to five main areas: system function, security strength or coverage, limitations, cost and research gaps.

System function refers to the primary security purpose of each system and the technologies employed. Security strength or coverage considers the type and combination of security mechanisms provided, including

authentication, intrusion detection, monitoring, vehicle identification, and notification. Limitations refer to constraints identified from the reviewed studies, such as dependence on network connectivity, processing requirements, hardware complexity, cost, or restricted application areas. System cost represents the approximate expenses required to develop, install, and operate each security system

The research gaps were identified by comparing the security functions and technologies provided by the selected systems. Particular attention was given to functions that were implemented separately rather than integrated into a single security platform. The comparison was used to identify opportunities for improving the integration of access control, intrusion detection, vehicle identification, monitoring, and notification in a proposed microcontroller-based security system for restricted buildings.

3.0 REVIEW OF EXISTING SECURITY SYSTEMS

The selected studies demonstrate that different technologies have been applied to address specific security requirements in buildings and other protected environments. These technologies include RFID, biometric authentication, sensors, cameras, machine learning, License Plate Recognition (LPR), IoT, cloud computing, and fog computing. The reviewed systems differ in their primary security functions, level of integration, processing requirements, and application areas. Table 3 summarizes the selected studies according to their principal function, security coverage, cost, limitations, and the gaps identified from the comparison.

Table 3: Comparative Analysis of Selected Security Systems

Author(s)	System/Technology	Main Function	Security Coverage	Cost	Major Limitation	Gap Identified from the Review
Oyedijiet al. (2025)	Microcontroller-Based Security Door Using RFID	RFID authentication and automatic door control	Medium	Low	Mainly addresses door access	Does not integrate intrusion detection and vehicle identification
Kishanet al. (2024)	RFID-Based Elevator Access Control System	Elevator access control using RFID/NFC and ESP32	Medium–High	Low–Moderate	Focuses mainly on elevator access	Limited coverage of wider building and perimeter security
Martín Toralet al. (2023)	OpenFog Smart-Building Architecture	Smart-building control and secure communication	High	Moderate–High	Architecture may increase system complexity	Limited emphasis on physical access control and intrusion detection
Al-Dooriet al. (2024)	RFID and Fingerprint Smart-Building Security	Combined RFID and fingerprint authentication	High	Moderate	Requires multiple authentication technologies	Does not address vehicle access and perimeter monitoring
Abdul-Rahaim& Mohammed (2025)	Cloud and RFID Security System	Multi-door access control and cloud monitoring	High	Moderate	Depends on cloud/network connectivity	Limited offline operation and intrusion monitoring
Arpilleda&Teleron (2025)	Smart Building Management System	Building security, energy, lighting, and operational monitoring	Medium–High	High	Broad building-management focus	Security functions are not specifically designed for restricted facilities
Prajoonet al. (2024)	E-Secure IoT Security System	Facial recognition, motion detection, gas detection, and remote access	High	Moderate	Primarily designed for residential environments	Limited suitability for high-security restricted buildings
Medhat et al. (2020)	IoT-Fog Smart-Building Security System	Intrusion, fire, and water-leakage detection	High	Moderate–High	Requires multiple computing components	Does not combine advanced access authentication and vehicle recognition
Abdellahet al. (2025)	Hybrid Indoor Security System	RFID, millimetre-wave radar, and facial recognition	Very High	High	Requires advanced sensors and processing hardware	High hardware and computational requirements may limit deployment in low-resource environments

Author(s)	System/Technology	Main Function	Security Coverage	Cost	Major Limitation	Gap Identified from the Review
Chen <i>et al.</i> (2021)	Blockchain-Based Community Safety Security System	IoT monitoring with blockchain-secured records	High	Moderate-High	Blockchain architecture increases complexity	Limited focus on direct physical access control for restricted buildings
Huda & Hakim (2025)	IoT-Based Visitor Identification Framework	Visitor identification using RFID, PIR, and Raspberry Pi	High	Low-Moderate	Mainly focuses on visitor identification	Does not combine vehicle access, perimeter intrusion detection, and SMS notification
Putluruet <i>al.</i> (2025)	YOLO-Based License Plate Recognition System	Vehicle detection and license-plate recognition	High	Moderate	Requires camera and substantial processing resources	LPR is not integrated with the broader building-security functions considered in this review
Ovioisa&Güney (2026)	IoT Smart Security System with Face and Object Detection	Facial and suspicious-object detection using machine learning	Very High	Moderate-High	May require substantial computational resources	Does not integrate vehicle authentication with physical access control
Çavaş& Ahmad (2018)	Design and Simulation of Four Walls Crossed Security System	Perimeter wall monitoring via LDR/LED sensors and CCTV rotation	High	Low	Relies on line-of-sight optical sensors sensitive to ambient light	Focuses exclusively on perimeter walls without electronic user access control
Adetoyi (2017)	Development of Smart Card Door Access Control System	Dual-factor smart card and PIN verification	Medium	Low	Relies on physical credentials prone to loss or sharing	Lacks wider perimeter intrusion monitoring or cloud integration
Adjayeet <i>al.</i> (2024)	Gate automation systems using access control mechanisms	Automated gate entry using access control hardware	Medium	Moderate	Focuses primarily on gate entry mechanisms	Lacks a comprehensive multi-zone defense kit covering interior and perimeter breaches simultaneously
Penicaet <i>al.</i> (2025)	Advancing Interoperable IoT-Based Access Control Systems	Interoperable physical access control gateway architecture	High	Moderate	Focuses primarily on gateway interoperability frameworks	Lacks a complete physical end-point kit for every type of entryway

4.0 DISCUSSION OF EXISTING SECURITY SYSTEMS

The reviewed studies demonstrate that recent building-security systems have increasingly adopted microcontrollers, radio frequency identification (RFID), biometric authentication, sensors, computer vision, machine learning, IoT, cloud computing, and fog computing. These technologies provide different security capabilities, but their functions, coverage, cost and implementation requirements vary considerably.

4.1 Single-Function Access Control Systems

RFID-based systems provide a straightforward approach to user authentication and automated access control. Oyedijiet *al.* (2025) developed an Arduino-based door system using RFID achieving a sensitivity rating of 78.57% and 91.9% accuracy with a 5-second auto-close delay, while Kishanet *al.* (2024) applied RFID/NFC with an ESP32 for elevator access control. Similarly, Adetoyi (2017) utilized a two-level smart card and PIN verification mechanism. However, these systems primarily address door or zone access and do not provide

comprehensive protection of the wider building perimeter.

4.2 Perimeter and Multi-Zone Intrusion Monitoring

Perimeter security relies heavily on sensors and automated tracking. Çavaş and Ahmad (2018) monitored four perimeter walls using LDR and LED sensors paired with a PIC microcontroller, achieving an estimated 96% reliability by rotating a CCTV camera toward breached walls. Medhat *et al.* (2020) implemented an IoT-fog-based smart-building security system using Arduino sensors and a Raspberry Pi edge node, reducing network usage by 71% and lowering latency compared to cloud solutions. Furthermore, Omedeet *al.* (2024) deployed a PIR sensor anti-burglar defense system achieving an average responsiveness of 83.56% via a triple-mode alert notification channel.

4.3 Multi-Modal and Biometric Integration

To heighten security strength, advanced systems combine multiple authentication layers. Al-Dooriet *al.* (2024) integrated RFID with fingerprint scanning to establish a dual-factor entry lock. Safyet *al.* (2025) combined UHF RFID, millimetre-wave radar (IWR1642), and YOLOv5-Tiny computer vision via a Kalman filter, increasing detection accuracy by 14%, reducing false positives by 22%, and maintaining a 24 FPS real-time performance using TensorRT edge acceleration. Similarly, Prajoonet *al.* (2024) integrated facial recognition guest authorization with gas and motion sensors via a Raspberry Pi.

4.4 Vehicle Identification and Cloud/Edge IoT Frameworks

Vehicle tracking and centralized network infrastructures have also been explored. Putluru *et al.* (2025) investigated a YOLO-based License Plate Recognition (LPR) system for vehicle detection, while Adjayeet *al.* (2024) integrated LPR, biometrics, and mobile technology for automated gate control. For distributed management, Abdul-Rahaim and Mohammed (2025) utilized an Arduino Uno connected via cloud/fog infrastructure for multi-door tracking. Addowet *al.* (2025) implemented an ESP32-controlled smart home automation system monitored via a Flutter app, and Arpilleda and Teleron (2025) developed an edge-computing smart building management system with usability ratings exceeding 4.6/5. Finally, Penicaet *al.* (2025) focused on interoperable IoT gateway architectures using a Raspberry Pi Compute Module CM3, while Wang *et al.* (2017) emphasized operating-system-level microkernel architectures (MINIX 3 and seL4) to isolate critical building automation processes.

5.0 IDENTIFIED RESEARCH GAP

The comparison of the selected studies reveals several gaps in existing approaches to building and restricted-area security:

5.1 Single Function Focus

Many of the reviewed systems concentrate strictly on a single security domain. For instance, Oyedijiet *al.* (2025) and Kishanet *al.* (2024) focus exclusively on access authentication, while Putluru *et al.* (2025) deal solely with vehicle license plate recognition without handling multi-zone security.

5.2 Separation of Access Control and Intrusion

Access control and perimeter intrusion detection are frequently treated as isolated functions. Systems like Çavaş and Ahmad (2018) or Medhat *et al.* (2020) monitor environmental or perimeter threats without integrating user biometric or smart card access control into the same platform.

5.3 Isolated Vehicle Identification

Vehicle identification via License Plate Recognition (LPR) operates independently from internal building security matrices (Putluru *et al.*, 2025), failing to feed vehicle data into a unified access decision framework.

5.4 Resource and Infrastructure Overheads

Advanced multi-sensor or machine-learning architectures (e.g., Safyet *al.*, 2025; Ovioisa&Güney, 2026) introduce heavy computational and processing requirements, making them less suitable for resource-constrained environments.

6.0 PROPOSED DIRECTION

Based on the insights and gaps identified in this review, several key directions are recommended for future research and development in microcontroller-based security systems for restricted buildings:

- i. **Integration of Multi-Modal Platforms:** Future designs should move away from single-function silos by integrating user authentication (such as RFID and biometrics), perimeter sensors, and vehicle identification (License Plate Recognition) into a single, unified hardware and software framework.
- ii. **Virtual Simulation and Prototyping:** Before committing to costly physical hardware deployments, future systems should utilize virtual simulation environments (such as Proteus, MATLAB/Simulink, or IoT cloud emulators) to rigorously test component-to-component interactions, latency limits, and edge-case response handling.

- iii. **Optimizing Resource-Constrained Edge Processing:** As advanced machine learning models and multi-sensor fusion algorithms are introduced, future work must focus on lightweight computing architectures (such as edge-fog node optimization) to ensure high performance without overwhelming the processing and power budgets of microcontrollers like the ESP32 or Arduino.
- iv. **Resilience Against Cyber-Physical Threats:** Future implementations should incorporate lightweight encryption, secure communication protocols, and firmware vulnerability assessments to mitigate IoT-specific risks like denial-of-service and unauthorized remote interception.

7.0 CONCLUSION

This paper has synthesized current developments in microcontroller-based and IoT-enabled security architectures for restricted facilities. Rather than merely reiterating descriptive findings, the comparative analysis of the 17 reviewed studies underscores a critical structural evolution in building security: while individual

technologies such as RFID, biometrics, LPR, and fog computing achieve high localized performance, their fragmentation creates systemic vulnerabilities.

The primary insight derived from this review is that the effectiveness of modern building security is constrained not by a lack of technological capability, but by a lack of architectural integration. Standalone systems force a trade off between granular authentication and comprehensive perimeter awareness. Consequently, future development must pivot toward unified frameworks that synthesize access control, intrusion detection, and vehicle identification into a single reactive platform.

Ultimately, this study establishes that employing virtual simulation environments is an essential methodological bridge. Simulation enables the rigorous pre-evaluation of multi-component interactions and edge-case responsiveness before physical deployment, thereby providing a scalable and cost-effective pathway for the next generation of intelligent, multi-functional security systems.

REFERENCE

- Abdellah, M. R., Nagm, A. M., Abdelhafeez, A., Ebrahim, M., & Safy, M. (2025). Hybrid indoor security system based on millimetre wave radar, RFID, and face recognition. *Statistics, Optimization & Information Computing*, 14(6), 3718–3740. <https://doi.org/10.19139/soic-2310-5070-2680>
- Abdul-Rahaim, L. A., & Mohammed, H. A. (2025). A multi-authority security system based on the cloud and radio frequency identification systems. In 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA) (pp. 1–6). IEEE. <https://doi.org/10.1109/ICHORA65333.2025.11017069>
- Adetoyi, O. E. (2017). Development of smart card door access control system. *International Journal of Electronics Communication and Computer Engineering*, 8(1), 41–44. https://ijecce.org/administrator/components/com_jresearch/files/publications/IJECCE_4071_FINAL.pdf
- Adjaye, A. I., Darko, D. E. N., Tei-Mensah, N. J., Kofi, K. S., Freitas, S. N. Y., & Korang, J. (2024). Gate automation systems using access control mechanisms. In 2024 IEEE 9th International Conference on Adaptive Science and Technology (ICAST) (pp. 1–6). IEEE. <https://doi.org/10.1109/ICAST61769.2024.10856499>
- Advait, R., Uditya, V. K., Hariharan, S., & Sangeetha, R. G. (2026). Automated vehicle access control system using license plate recognition. *Scientific Reports*, 16, 21745. <https://doi.org/10.1038/s41598-026-47210-5>
- Ahanger, T. A., Tariq, U., Ibrahim, A., Ullah, I., & Bouteraa, Y. (2020). IoT-inspired framework of intruder detection for smart home security systems. *Electronics*, 9(9), 1361. <https://doi.org/10.3390/electronics9091361>
- Al-Doori, V. S., Maktoof, M. A. J., Abdulqader, A. F., & Lienkov, S. (2024). Securing smart buildings using RFID and fingerprint technologies. In 2024 35th Conference of Open Innovations Association (FRUCT) (pp. 71–81). IEEE. <https://doi.org/10.23919/FRUCT61870.2024.10516379>
- Arjun, S., GopiKrishna, V., Gowtham, B., Siddharthan, B., & Manikandan, V. (2023). Smart home security analysis using microcontroller. *IRO Journal on Sustainable Wireless Systems*, 5(2), 108–120. <https://doi.org/10.36548/jsws.2023.2.003>
- Arpilleda, J. Y., & Teleron, J. I. (2025). Design and implementation of a smart building management system using edge computing technologies. In 2025 International Conference on Computer and Applications (ICCA) (pp. 1–6). IEEE. <https://doi.org/10.1109/ICCA66035.2025.11430825>
- Bashir, M. R., Gill, A. Q., & Beydoun, G. (2022). A reference architecture for IoT-enabled smart buildings. *SN Computer Science*, 3, 493. <https://doi.org/10.1007/s42979-022-01401-9>

IJSGS FUGUSAU VOL. 12 (3)	WEBSITE: https://fugus-ijsgs.com.ng
Bhardwaj, A., Bharany, S., Abulfaraj, A. W., Ibrahim, A. O., & Nagmeldin, W. (2024). Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities. <i>Egyptian Informatics Journal</i>, 25, 100443. https://doi.org/10.1016/j.eij.2024.100443 Çavaş, M., & Ahmad, M. B. (2018). Design and simulation of four walls crossed security system against intrusion using PIC microcontroller. <i>American Journal of Engineering Research (AJER)</i>, 7(12), 233–244. https://www.ajer.org/papers/Vol-7-issue-12/ZD0712233244.pdf Chen, C.-L., Lim, Z.-Y., & Liao, H.-C. (2021). Blockchain-based community safety security system with IoT secure devices. <i>Sustainability</i>, 13(24), 13994. https://doi.org/10.3390/su132413994 Graveto, V., Cruz, T. J., & Simões, P. (2022). Security of building automation and control systems: Survey and future research directions. <i>Computers & Security</i>, 112, 102527. https://doi.org/10.1016/j.cose.2021.102527 Huang, Y., Fu, B., Peng, N., Ba, Y., Liu, X., & Zhang, S. (2022). RFID authentication system based on user biometric information. <i>Applied Sciences</i>, 12(24), 12865. https://doi.org/10.3390/app122412865 Huda, C., & Hakim, L. (2025). Optimizing security with an IoT: A data-driven visitor identification framework. <i>Jurnal Teknologi Informasi dan Terapan</i>, 12(2), 163–170. https://doi.org/10.25047/jtit.v12i2.421 Kia, A., Storey, A. W., & Imtiaz, M. (2026). Advanced hardware security on embedded processors: A 2026 systematic review. <i>Electronics</i>, 15(5), 1135. https://doi.org/10.3390/electronics15051135 Kishan, S. R., Hameed, S., Charan, J., & Srikar, Y. (2024). RFID-based elevator access control system. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1–5). IEEE. https://doi.org/10.1109/ICCCNT61001.2024.10724057 Martín Toral, I., Calvo, I., Xenakis, J., Artetxe, E., & Barambones, O. (2023). Architecture for smart buildings based on fuzzy logic and the OpenFog standard. <i>Electronics</i>, 12(24), 4889. https://doi.org/10.3390/electronics12244889 Medhat, M., El-Shafey, K., & Rashed, A. (2020). IoT-Fog based smart-building security system design and performance evaluation. <i>Journal of Computer Science</i>, 16(9), 1325–1333. https://doi.org/10.3844/jcssp.2020.1325.1333 Murthy, A., Asghar, M. R., & Tu, W. (2024). A lightweight intrusion detection for Internet of Things-based smart buildings. <i>Security and Privacy</i>, 7(4), e386. https://doi.org/10.1002/spy2.386	Ovioisa, B., & Güney, H. (2026). Internet of Things-based smart security system with face and object detection using machine learning. <i>Sakarya University Journal of Computer and Information Sciences</i>, 9(3), 896–919. https://doi.org/10.35377/saucis.1805817 Oyediji, F. T., Oyebiyi, A. J., & Olaleke, M. O. (2025). Construction of a microcontroller based security door system using Radio Frequency Identification (RFID). <i>SSR Journal of Engineering and Technology</i>, 2(2), 30–38. https://doi.org/10.5281/zenodo.16259060 Pal, S., & Jadidi, Z. (2021). Protocol-based and hybrid access control for the IoT: Approaches and research opportunities. <i>Sensors</i>, 21(20), 6832. https://doi.org/10.3390/s21206832 Penica, M., Bhattacharya, M., O'Brien, W., McGrath, S., Hayes, M., & O'Connell, E. (2025). Advancing interoperable IoT-based access control systems: A unified security approach in diverse environments. <i>IEEE Access</i>, 13, 27767–27782. https://doi.org/10.1109/ACCESS.2025.3538748 Pilotti, F., Pavone, A., Di Sabatino Farinelli, L., Tinelli, S., & Paolone, G. (2026). AIoT-based security systems for smart homes and smart buildings: A tertiary study. <i>Future Internet</i>, 18(6), 307. https://doi.org/10.3390/fi18060307 Prajoon, P., Paul, A., Aswin, M. P., Athul, P. S., & Mohan, N. (2024). E-Secure: Security system using IoT. In 2024 International Conference on Advancement in Renewable Energy and Intelligent Systems (AREIS) (pp. 1–5). IEEE. https://doi.org/10.1109/AREIS62559.2024.10893679 Putluru, A. R., Pannuru, V. R., Ashok Kumar, C., & Kumar, C. J. (2025). An optimized YOLO-based license plate recognition system with integrated privacy safeguards. In 2025 2nd International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1053–1060). IEEE. https://doi.org/10.1109/ICMLAS64557.2025.10968016 Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. <i>Electronics</i>, 13(16), 3343. https://doi.org/10.3390/electronics13163343