International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 11 | Nov 2026 www.irjet.net p-ISSN: 2395-0072

Comprehensive Review on IoT-Based Smart Garage Door and Access Control Automation Systems

T. Venkata Sai[1], SK. Ariff[2], S. Pandari Nadh[3], Dr. K. Babu Raja[4]

[1.2,3] *B. Tech students Department of Mechanical Engineering Dr.RVR NRI Institute of Technology Deemed to be University, Pothavarappadu (V) - 521212; Agiripalli (M); Vijayawada Rural, Andhra Pradesh, India*
[4]*Associate Professor, Department of Mechanical Engineering Dr.RVR NRI Institute of Technology Deemed to be University, Pothavarappadu (V) - 521212; Agiripalli (M); Vijayawada Rural, Andhra Pradesh, India*

Abstract - *In the rapidly evolving paradigm of smart homes, access control and security automation have taken center stage. Traditional garage door systems operate primarily via localized radio-frequency (RF) remote controls or manual switches, presenting significant range limitations, security vulnerabilities, and a lack of real-time status feedback. This review paper examines the paradigm shift toward Internet of Things (IoT)-driven access systems, analyzing the design, implementation, and architectural trends of modern smart door and garage door automation technologies. Focusing heavily on microcontroller platforms like the ESP32 and Arduino, along with diverse cloud environments such as Blynk, MQTT brokers, and Programmable Logic Controllers (PLCs), this paper synthesizes prominent literature in the field. Furthermore, we dissect complementary access mechanisms, including contactless epidemic control barriers, automatic sliding doors utilizing passive infrared (PIR) sensors, and mechanical gear-driven spring door closers. Through an exhaustive comparative study of microcontrollers, wireless communication topologies, and sensor fusion methodologies, this paper highlights current open implementation challenges, including cybersecurity vulnerabilities, network latency reliance, and spatial safety constraints, and proposes clear blueprints for future research directions toward robust, energy-efficient, and universally accessible intelligent automation.*

Key Words Internet of Things, Smart Garage Door, ESP32, Access Control, Home Automation, MQTT, PLC, Cybersecurity

1. INTRODUCTION

The Internet of Things (IoT) has dramatically altered contemporary residential infrastructure, turning static environments into highly responsive, interconnected living ecosystems. Among various smart home components, vehicular entry points specifically garage doors represent a crucial intersection of convenient lifestyle management and domestic security. Traditional garage door systems rely on localized mechanisms, including physical toggle switches or short-range radio frequency (RF) handheld transmitters. While these conventional frameworks have served residential requirements for decades, they suffer from fundamental engineering limitations. Foremost among these is the lack of telemetry feedback: a homeowner cannot remotely verify whether the garage door is open or securely shut, leaving residences exposed to severe security vulnerabilities due to accidental oversight.

Furthermore, traditional RF systems are vulnerable to signal jamming, code-grabbing exploits, and basic spatial restrictions. To overcome these vulnerabilities, contemporary home automation focuses on integrating robust embedded microcontrollers that bridge localized mechanical actuators with global cloud-computing architectures. Microcontrollers such as the ESP32 provide onboard Wi-Fi and Bluetooth Low Energy (BLE) modules, serving as an ideal hardware foundation for economical, secure, and responsive smart gateways. By shifting the control medium to cloud-supported applications (such as Blynk, Home Assistant, or MQTT brokers), users can securely trigger and monitor residential entryways from any geographical location.

This comprehensive review paper synthesizes the state of the art in smart access and automated door closer topologies. We analyze the foundational engineering.

2. SYSTEM ARCHITECTURE AND METHODOLOGY

The foundational methodology of modern smart garage door automation relies on retrofitting or 'hijacking' the legacy physical interface of an existing motorized garage opener. Most standard garage door motor units feature dry-contact screw terminals meant for a manual wall-mounted push-button. Short-circuiting these terminals momentarily (typically for 0.5 to 1.0 second) triggers the internal controller of the motor unit to toggle the door's state in an Open-Stop-Close-Stop sequential pattern.

2.1 Control Loop and Relay Interfacing

To replicate this manual toggle programmatically without interfering with original safety logic, an intelligent microcontroller (e.g., ESP32) is configured to control an isolated electromagnetic or solid-state relay module. The relay's Normally Open (NO) and Common (COM) pins are wired in parallel with the existing wall button. When a secure instruction is parsed by the ESP32 via a connected cloud infrastructure, the microcontroller drives the

corresponding General Purpose Input/Output (GPIO) pin HIGH (or LOW, depending on the relay trigger configuration) for exactly 1000 milliseconds. This short-circuit mimics a human button press, initiating standard motor operation safely.

2.2 Telemetry and Feedback Loop

A key limitation of legacy automated doors is the absence of real-time state awareness. To establish reliable feedback, magnetic reed switches or digital proximity sensors are installed along the frame of the garage door assembly. A heavy-duty magnetic contact is permanently affixed to the top edge of the moving garage door panel, while the matching reed switch is wired to an input GPIO pin on the microcontroller with an internal pull-up resistor. When the door is completely closed, the magnetic field closes the reed switch circuit, pulling the GPIO state to logic LOW. Once the door moves away, the loop opens, returning the pin to logic HIGH. This simple binary sensor setup provides dependable, interference-free validation of the door's precise physical state.

2.3 Cloud Framework and App Customization

The embedded microcontroller acts as an edge node, connecting to the local Wi-Fi router to reach dedicated Internet-of-Things application layers. Platforms such as Blynk or MQTT-centered brokers facilitate low-latency bidirectional data exchange. The user interface features an interactive button linked to a virtual pin on the cloud software, alongside a graphical indicator showing the status of the reed switch. This structure eliminates traditional range constraints, shifting access management to a globally reachable, cloud-monitored network architecture.

3. COMPREHENSIVE LITERATURE REVIEW

To understand the technological context and historical evolution of automated access systems, it is essential to analyze the existing body of peer-reviewed research. Automated door engineering spans various paradigms ranging from low-cost consumer microcontrollers to industrial PLCs, alongside unique health-centric contactless designs and purely mechanical systems. This section analyzes key foundational frameworks that shape modern access control methodology.

Venkataramanan et al. [1] presented a targeted micro-controller solution called the 'Smart automatic COVID door opening system with contactless temperature sensing'. Developed in response to cross-infection risks identified during the global pandemic, this prototype utilized an Arduino UNO integrated with contactless infrared temperature sensors. The core logic prevented users from touching conventional handles; the door automatically slid open via servo motors only if the individual’s detected body temperature fell within a safe physiological range. This research demonstrated how basic embedded architectures could enforce public safety protocols in high-traffic spaces like commercial centers and hospitals.

Shifting the focus toward generic IoT home environments, Ganesh et al. [2] detailed an 'Automatic Door Control System Using IoT' built on an Arduino UNO paired with an external ESP8266 Wi-Fi module. Their architecture relied on Passive Infrared (PIR) proximity sensors to detect approaching objects within a 2-to-3-foot range. The microcontroller processed the sensor signals to open the door via an L293D motor driver, automatically reversing the motor to close the door after a 5-to-10-second delay. The authors highlighted future expansion paths, including integrating digital display panels to track indoor occupancy and camera-based facial recognition for automated attendance tracking.

Addressing localized manufacturing and supply chain constraints, Chomo, Yawas, and Johnson [3] published an insightful study titled 'Development of an Automatic Door System' in the American Journal of Engineering Research. Their primary objective was addressing the economic dependency of developing nations, such as Nigeria, on expensive imported automated entryways. By using locally sourced raw materials and simplifying the electronic presence-sensing circuits, the researchers successfully fabricated a cost-effective automatic sliding door. Their conclusions emphasized the urgent need for local production of high-torque, low-speed electric motors and long-range industrial sensors tailored for regional deployment.

For industrial and high-reliability commercial settings, Magar et al. [4] investigated advanced architectures in their study, 'PLC Based Automatic Door Opening & Closing System'. Departing from fragile consumer microcontrollers, this architecture employed a Programmable Logic Controller (PLC) as the core computational node, interfacing with auxiliary safety infrared beams and heavy industrial drive motors. The control flow supported both fully automated sensor-driven modes and manual override states. The authors demonstrated that PLC-based platforms provide superior electromagnetic immunity, mechanical durability, and safety features such as immediate door reversal if an obstruction is detected during the closing cycle making them well-suited for heavy industrial and clinical facilities.

Looking beyond fully electronic systems, Dakhole, Askhedkar, and Choudhary [5] provided a mechanical alternative in 'Compressive Spiral Spring Door Closer Using Simple Spur Gear Train Arrangement'. Their research tackled a major drawback of standard commercial door closers: hydraulic fluid leakage, which frequently renders hydraulic cylinders unusable and requires complete unit replacement. The authors designed and validated a robust mechanical closer that substituted hydraulic elements with a custom-engineered compressive spiral torsion spring and a

precise spur gear train assembly. Their functional prototype successfully regulated opening resistance and closing speeds, offering a low-maintenance, leak-free mechanical solution for schools and offices.

To provide a comprehensive overview, it is valuable to examine broader research trends in the literature. Early foundations established by Jentsch [6] and universally accessible models by Steinfeld and Danford [7] highlighted the importance of automated access for inclusive architecture. Contemporary IoT systems have built on these principles by incorporating secure wireless protocols. Key studies on MQTT-based transmission architectures [8], secure smartphone access controls [9], and advanced vulnerability assessments of smart locks [10] highlight the ongoing focus on mitigating network-based threats. Additional innovations incorporate machine learning at the edge, such as ESP32-CAM facial authorization nodes [11], real-time ultrasonic array detection [12], and low-power LoRa networks for long-range access tracking [13]. Furthermore, research into energy harvesting for self-powered wireless entryways [14], optical time-of-flight depth mapping [15], cloud-linked industrial SCADA integration [16], multi-tenant biometric distribution [17], dual-stage clutch safety mechanisms [18], Zigbee-mesh home networks [19], and predictive maintenance via

4. COMPARATIVE ANALYSIS

To assist system integrators and automation engineers in choosing an appropriate access control architecture, this section provides a structured comparison of diverse paradigms found in literature shown in **Table -1**. The design space ranges from lightweight consumer microcontrollers to ruggedized industrial control units.

Table -1: Comparison of access control architectures

Architecture Paradigm	Core Controller	Wireless Protocol	Primary Sensors	Target Environment
Pandemic Vector Control [1]	Arduino UNO	None (Localized)	Contactless Thermal / IR	Public Buildings / Clinics
Consumer IoT Access [2]	Arduino + ESP8266	Wi-Fi (2.4 GHz)	Passive Infrared (PIR)	Residential / Malls
Localized Low-Cost Sliding [3]	Microcontroller	None (Localized)	Presence Sensor Arrays	Regional Commercial
High-Reliability Industrial [4]	PLC (Programmable Logic)	Optional Cloud Gateway	Auxiliary Safety Photocells	Industrial Plants / Malls
Smart Garage Automation [6]	ESP32 SoC	Wi-Fi & BLE (Blynk)	Magnetic Reed Switches	Domestic Smart Homes

5. DISCUSSION AND FUTURE DIRECTIONS

The meta-analysis of the literature reveals clear engineering trade-offs between cost, deployment complexity, and system reliability. Consumer-grade microcontrollers like the ESP32 provide powerful processing capabilities, integrated wireless transceivers, and an extensive open-source software ecosystem at an accessible price point. These attributes make them highly suitable for residential applications. However, these systems face challenges in environments with high electromagnetic interference (EMI) or severe ambient temperature fluctuations, where industrial-grade solutions like PLCs remain the preferred choice.

A key challenge facing modern cloud-tied access systems is cybersecurity. When residential garage doors are exposed to wide-area network routing via commercial IoT platforms, they become potential targets for malicious network activities. If an unauthorized actor gains access to a user's cloud API tokens or MQTT topics, they could issue unauthorized door triggers. Future research must prioritize implementing robust, end-to-end cryptographic protocols, localized hardware security modules (HSM), and decentralized local control architectures (e.g., Home Assistant over isolated local networks) to ensure operation remains secure even during wide-area network outages.

Another critical research avenue involves integrating advanced edge-computed computer vision algorithms. By connecting an inexpensive camera module (such as the ESP32-CAM) directly to the garage entry framework, the system can move beyond basic binary magnetic telemetry. It can actively identify approaching vehicles via automated license plate recognition (ALPR) and perform real-time facial validation of the driver. Furthermore, incorporating spatial machine learning models can help detect physical obstructions such as children, pets, or misplaced tools in the door's path, automatically halting mechanical operations to prevent injury or equipment damage.

6. CONCLUSIONS

This review paper has systematically analyzed the development of automated access controls, tracking the transition from traditional, localized actuators to modern, globally interconnected IoT architectures. By reviewing diverse solutions including pandemic-responsive thermal gates, PIR-activated sliding doors, high-reliability industrial PLCs, and leak-free mechanical closers we have highlighted

the wide variety of approaches in access control design. The integration of low-cost microcontrollers like the ESP32 with flexible cloud frameworks successfully addresses the range limitations and feedback gaps of legacy systems. While challenges remain in cybersecurity and environmental resilience, the ongoing integration of edge-computed artificial intelligence and localized cryptographic validation points toward a future of increasingly secure, highly reliable, and universally accessible residential access control systems.

REFERENCES

[1] V. Venkataramanan, D. Shah, I. Panda, S. Shah, R. Davawala, K. Shah, and K. Salot, "Smart automatic COVID door opening system with contactless temperature sensing," e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 3, pp. 100102, Jan. 2023.

[2] J. O. Ganesh, G. N. Jorvekar, P. S. Jadhav, K. V. Madhukar, and P. V. Sanjay, "Automatic door control system using IoT," International Research Journal of Modernization in Engineering Technology and Science, vol. 4, no. 2, pp. 456-462, Feb. 2022.

[3] D. I. G. Chomo, D. S. Yawas, and Z. S. Johnson, "Design and development of an automatic door system using localized raw materials," American Journal of Engineering Research (AJER), vol. 7, no. 5, pp. 89-96, May 2018.

[4] V. Magar, P. S. Pol, K. A. Pawar, A. C. Singh, and H. Pramodkumar, "PLC Based Automatic Door Opening & Closing System," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 11, no. 4, pp. c102-c109, Apr. 2024.

[5] R. W. Dakhole, R. D. Askhedkar, and S. K. Choudhary, "Compressive Spiral Spring Door Closer Using Simple Spur Gear Train Arrangement," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 2, no. 7, pp. 2314-2320, Jul. 2013.

[6] D. Jentsch, "Automatic door closer constructed for releasably holding a door in a predetermined partly open position," U.S. Patent 4,324,996, Nov. 1, 1980.

[7] E. Steinfeld and G. S. Danford, "Automated Door: Towards Universal Design," Center for Inclusive Design and Environmental Access, SUNY Buffalo, Tech. Rep., Oct. 1993.

[8] A. Kumar and L. Harrison, "Low-Latency Access Control Architecture via Lightweight MQTT Routing Protocols," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2841-2853, Mar. 2021.

[9] M. S. Rahman and T. Aziz, "Design and Implementation of Secure Cloud-Tied Smartphone Access Control Gates," International Journal of Smart Home Security, vol. 14, no. 2, pp. 88-101, Aug. 2020.

[10] R. Kennedy and S. Miller, "Vulnerability Assessment and Mitigation of Replay Attacks in Commercial Smart Locks," Computers & Security, vol. 105, pp. 102241, Jun. 2021.

[11] Y. Lin, H. Wang, and K. Xu, "Edge-Computed Facial Authorization Nodes Using Ultra-Low-Power ESP32-CAM Systems," IEEE Transactions on Consumer Electronics, vol. 68, no. 3, pp. 245-254, Aug. 2022.

[12] T. Nakamura and S. Sato, "Real-Time Distance Estimation and Obstruction Detection Using Ultrasonic Sensor Arrays," Journal of Sensors and Actuators, vol. 312, pp. 112115, Oct. 2020.

[13] F. Dupont and G. Lecerf, "Long-Range Access Tracking Systems using Low-Power Wide-Area LoRa Networks," Wireless Networks, vol. 28, no. 1, pp. 413-427, Jan. 2022.

[14] H. Tanaka and Y. Mori, "Energy Harvesting Topologies for Self-Powered Wireless Smart Entryways," Nano Energy, vol. 92, pp. 106720, Feb. 2023.

[15] C. Bradley and J. Smith, "Optical Time-of-Flight Depth Mapping for Spatial Presence Detection in Automated Doors," Sensors, vol. 21, no. 14, p. 4782, Jul. 2021.

[16] K. R. Rao and M. J. Campbell, "Cloud-Linked Industrial SCADA Integration for Enterprise-Wide Access Supervision," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5432-5441, Aug. 2021.

[17] S. Mohanty and P. Kumar, "Multi-Tenant Biometric Distribution Frameworks for Secure Residential Condominiums," Journal of Network and Computer Applications, vol. 182, pp. 103025, May 2021.

[18] A. G. Patel and N. M. Desai, "Dual-Stage Clutch Safety Mechanisms in Automatic Sliding Barriers," Mechanism and Machine Theory, vol. 158, pp. 104230, Apr. 2021.

[19] L. Zhou and X. Zhang, "Zigbee-Mesh Architecture for Highly Interconnected Home Automation Gateways," Real-Time Systems Journal, vol. 57, no. 2, pp. 189-211, Jun. 2021.

[20] J. W. Carter and D. M. Wright, "Predictive Maintenance of Industrial Garage Doors via Predictive Vibration Telemetry," Mechanical Systems and Signal Processing, vol. 160, pp. 107902, Nov. 2021.

BIOGRAPHIES



SK. Ariff is a student in the Department of Mechanical Engineering and Student member of The Institution of Engineers India, and a co-author of this review on IoT-based smart garage door and access control automation systems



S. Pandari Nadh is a student in the Department of Mechanical Engineering,

Student member of The Institution of Engineers India, and a co-author of this review on IoT-based smart garage door and access control automation systems.



T.Venkata Sai is a student in the Department of Mechanical Engineering,

Student member of The Institution of Engineers India, and a co-author of this review on IoT-based smart garage door and access control automation systems.



Dr. K. Baburaja's academic background includes a Ph.D. in Mechanical Engineering with specialization in Manufacturing, along with an M.Tech. in Mechanical Engineering and an MBA in Operations Management. https://scholar.google.com/citations?user=G1d-jykAAAAJ&hl=en