Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Secure Offline Smart Office Automation System Using ESP32 and Bluetooth Control Architecture

Mahmood A. Al-Shareeda[1, 2], Ahmed Nader jafer[3], Mohammed Tahseen Hashem [3], Murtaza Salman Fajr[3]

[1] *Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq*
[2] *Communication Engineering, Iraq University College, Basra, Iraq*
[3] *Computer Technology Engineering, Iraq University College, Basra, Iraq*

ARTICLE INFO

Academic Editor:
Prof. Youakim Badr

Vol.2024, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2024.1.2

ABSTRACT

This paper describes the development and deployment of an affordable and secure smart office automation system which is completely offline and it use Bluetooth technology and ESP32 microcontroller. In situations where internet access is limited or security is of utmost concern, the system provides an app-based control over the office devices like lighting, blinds, door access and alert systems, in real- time. The design eliminates dependence on the cloud, which in turn mitigates security threats from the outside, meanwhile, local Bluetooth communication shortens response time and cuts power consumption. Primary security requirements are direct device linking, local command control and encryption-capable communication protocols. Experimental results substantiate quick response of devices (<150) ms, low power consumption and robustness in the indoor range of Bluetooth (10 m). The device is designed to be modular to enable extension of the system itself including however not limited to environmental sensors, GUI based mobile applications and cutting edge authentication protocols. This paper presents proof to ant small-to-medium sized enterprises about the availability of a secure and offline smart office system which is cost-effective, user-friendly and immune against security threats from outside.

Keywords: Smart Office Automation; ESP32 Microcontroller; Bluetooth Communication; Offline Control Systems; Embedded Security; Low-Cost IoT Architecture; Secure Device Control; Internet-Free Automation; Office Access Management; Energy-Efficient Automation.

How to cite the article
Al-Shareeda, M. A., Jafer, A. N., Hashem, M. T., & Fajr, M. S. (2024). Secure Offline Smart Office Automation System Using ESP32 and Bluetooth Control Architecture. Journal of Cyber Security and Risk Auditing, 2024(1), 3–13. https://doi.org/10.63180/jcsra.thestap.2024.1.2

**Corresponding author. Email:* *mahmood.alshareedah@stu.edu.iq*

1. Introduction

As we enter the digital age of office automation, increasingly intelligent solutions revolutionize the office landscape, allowing real-time monitoring, and energy saving, and improved user comfort [1–3]. Among these systems, Smart Office Automation Systems have attracted substantial interest due to their potential to simplify device control and conserve energy using technologies such as the Internet of Things (IoT), cloud computing, and wireless communication [4–6]. But some current systems depend on the 'always on' connection S2 and third-party cloud services S3, exposing privacy issues, potential security breaches and system downtime [7, 8].

While cloud resources provide flexibility and elasticity they also come with associated risks i.e. unauthorized access, data being intercepted and services being blocked. Or if your organization exists in a high-security environment, or doesn't have access to internet connections, alternative smart office solutions should be able to work without reliance on the Internet yet still be effective and responsive[9–11].

In this paper, we describe a safe, offline smart office automation system using the ESP32 microcontroller as well as Bluetooth connectivity. Our approach deviates from the standard topologies that rely on a cloud service or a Wi-Fi connection for control of office devices, and instead provides a local, encrypted connection to power devices in a office through a smartphone application, using Bluetooth Serial communication. Without the need for internet access, the solution reduces external attack surfaces and can operate reliably in secured environments.

The proposed system uses a modular architecture and it is portable, low cost and easy to use and manage several devices like lighting, fan, door access (servo motor), and buzzer notifications. We focus on security features like device pairing directly to the device, tap to join Wi-Fi, and the option to support future, encrypted protocols or biometric authorizations. It is a perfect solution for small and medium businesses, schools, and private offices that want to automate but lack the budget for expensive, complex systems.

Alongside the system design, this paper demonstrates experiments assessing the response times of the devices, its power requirements and Bluetooth range for communication. The architecture can also be extended in the future with environmental sensors and Wi-Fi/cloud modules (while still not losing sight of security). The contributions of this paper are:

- Design of smart office system based on ESP32 and Bluetooth with offline security without internet dependence.
- Realization of device oriented automation and access through local control infrastructure.
- Hardware Evaluations of system latencies, message reliabilities, and leakage power.

- Bluetooth, smart office and security: discussing the advantages and challenges of a security-aware office environment.

The remainder of this paper is organized as follows: In Section 2, related works in smart automation systems is surveyed. System architecture, hardware and software integration are described in section 3. Section 4 contains the implementation results and performance measures. Section 5 concludes and describes future work to extend the approach.

2. Related Works

Automated environment has a burgeoning growth, especially in home such as office automation, over the past few years. New technologies like Wi-Fi, Bluetooth, ZigBee, and cloud-based platforms have put in place the systems for lighting, climate, security, and energy management. Unfortunately, most of these systems are reliant on the internet, leading to security, dependability, and cost issues—especially in the context of sensitive and infrastructure-challenged environments [12, 13].

Siswanto et al. [14] developed a secure smart office prototype using face recognition and the ESP32 platform for room access. It highlights local security implementations and hardware-level efficiency for secure automation systems. Irugalbandara et al. [15] focuses on an ESP32 Node MCU system that runs entirely offline with secure command processing and energy monitoring—very aligned with your architecture. Litayem et al. [16] presents a security-optimized ESP32 system with offline functionality and modular IoT architecture, discussing BLE vs Wi-Fi control in constrained environments. Jion et al. [17] Implemented ESP32-CAM with digital door locks and secure mobile access. Useful for comparing access control mechanisms. Sauter [18] Investigates secure and offline control methods for building systems using lightweight encryption—good theoretical grounding for your offline Bluetooth control.

 ISSN: 3079-5354

While there are many studies on automation through Arduino or Raspberry Pi with Wi-Fi or Bluetooth modules, there are few studies which explicitly address security- aware, offline, and modular smart office systems. With a few exceptions, these works assume uninterrupted internet access or disregard security methods such as encryption and user authentication. In addition, empirical results of performance measures – like round trip times, energy consumption, and device control granularity – are frequently underreported.

3. Methodology and System Architecture

3.1 Design Objectives

The design of the proposed system follows a modular and layered approach to achieve the following goals:
• Offline operability to ensure independence from cloud servers and internet access.
• Secure communication using Bluetooth Serial (ESP32-based).
• Scalable architecture for controlling multiple office assets (lighting, ventilation, doors).
• User-friendly interface through a mobile application.
• Low-power consumption using the ESP32's energy-efficient architecture.
The system is intended for deployment in small to medium-sized office environments, especially where data security or poor internet connectivity is a concern.

3.2 System Overview

As shown in Figure 1, the architecture integrates three core layers:

• Application Layer: An Android mobile application built using MIT App Inventor is used for sending control commands (ON/OFF/TOGGLE) to the ESP32 via Bluetooth.
• Control Layer: The ESP32 microcontroller functions as the central controller. It listens for Bluetooth input and triggers specific I/O pins mapped to actuators.
• Device Layer: Physical components include: Lights/Fans (relay-controlled); Servo Motor (for smart door access); and Buzzer (for alert notifications).

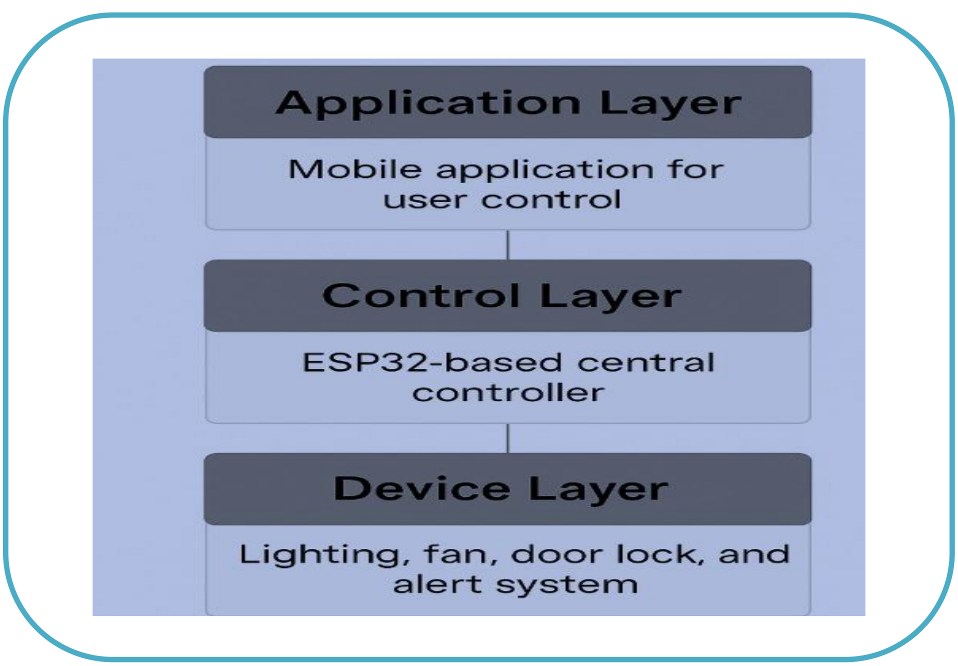


Figure 1. System Overview

ISSN: 3079-5354

4. Implementation and Experimental Setup

4.1 System Integration and Configuration

The design and realization of the designed smart office automation system was devel- oped using ESP32 microcontroller for the central processor. The ESP32 was selected for its built-in Bluetooth and Wi-Fi capabilities, strong GPIO support, low power needs, and good community support. As show in Figure 2, the system is implemented with the hardware modules listed below: ESP32 DevKit v1: main controller TongRui TR-D4: pump; HC-05 Bluetooth Module (or built-in BLE on native ESP32): for wireless serial communication; Relay Module (4-channel): to control AC appliances such as lights and fans; SG90 Servo x1: for smart lock mechanism; LEDs: with LED indicators to simulate lighting control and system status; Piezo Buzzers: Auditory alerts for either Door Access or Warnings; Smartphone: for sending commands on the mobile app.

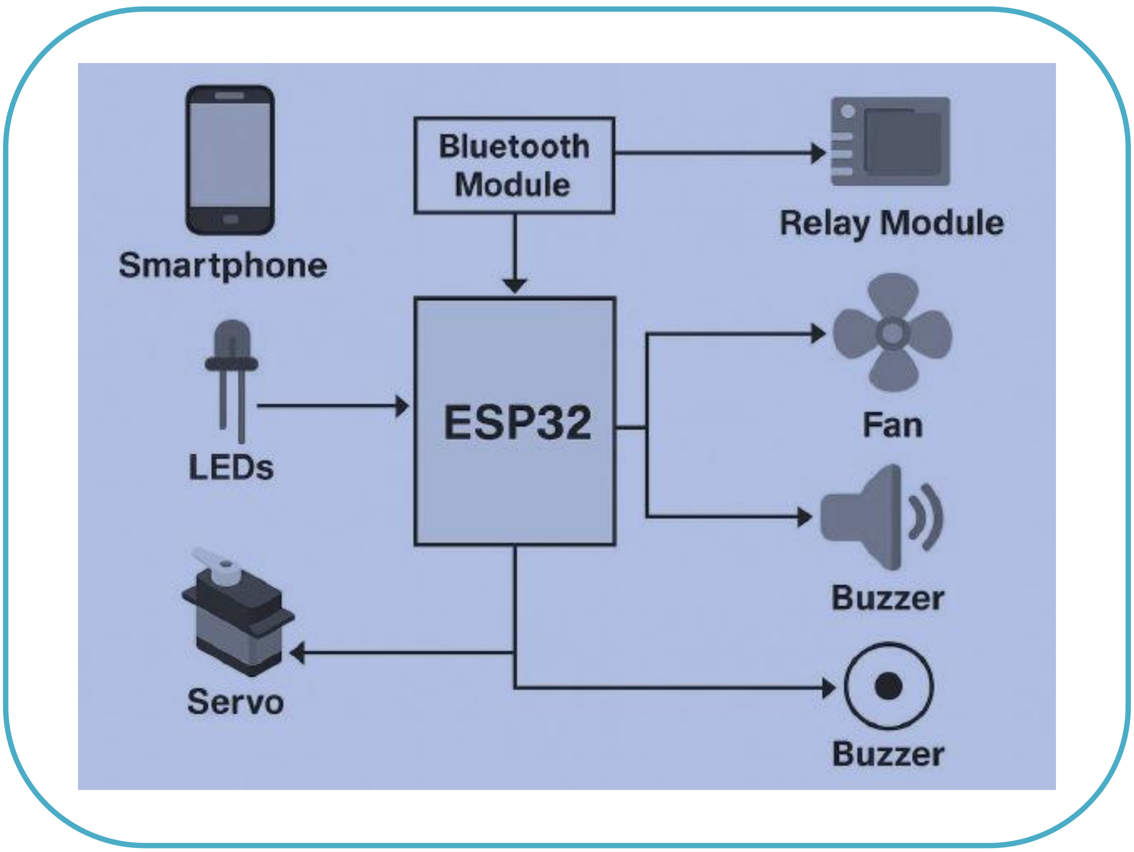


Figure 2. System Integration

The system was an autonomous one, which ran off a regulated 5V/2A DC power adaptor and was set up on a breadboard (for prototyping) followed by a more stable circuit (joint using solder) for experimental evaluation. The secure offline smart office automation prototype using ESP32 microcontroller and Bluetooth communication is presented in the figure above. The left image shows a top-down perspective of the office-like environment which showcases interior furniture and all components with integrated hardware. As depicted in Figure 3. A smartphone is presented that wirelessly communicates with the ESP32 through Bluetooth communication and controls the device on real-time basis via the custom control application. ESP32 board is interfaced to a relay module, servo motor, buzzer and LEDs with a regulated DC source as power supply. The bottom half of the setup shows the nicely packed circuit with stacked battery banks and jumper cabling for the ESP32 and its accessories.

 ISSN: 3079-5354

In the second image to the right, you can see the electrically servo-actuated smart door here in the open position. The door hinge is installed on the base and coupled to the servo motor to achieve a purpose of automatic access control. This physical integration successfully validates real-time actuation via secure Bluetooth command transmission from the smartphones. The image is to emulate an office lobby, proving that the prototype can deal with both physical security and internal environment control even when entirely offline.

Figure 3. Real Implementation

4.2 Development of Mobile App

A user-friendly GUI-based mobile app using MIT App Inventor incorporated command buttons for: Device ON/OFF toggling; Servo open/close control; Buzzer activation; and Toast feedback (simple toast messages). After manual connecting you have a Bluetooth Serial link to your ESP32. The commands are sent as ASCII values (e.g., A for fan ON, B for fan OFF) and conditioned using logic in the ESP32 firmware.

4.3 Firmware Programming

The ESP32 was programmed in Arduino ID with the following libraries: Bluetooth- Serial. h - for serial input through Bluetooth; Servo. h – to control the movement of the door lock; and Custom control routines for relays so on and output pins.

ISSN: 3079-5354

5. Results and Performance Evaluation

In this section, we showcase the gathered performance measurements over multi- ple experiments in the offline, Bluetooth-operated smart office automation system. Response time, transmission range, power consumption, and system reliability in an office environment are the key aspects examined.

5.1 Response Time Evaluation

The response performance (from the time the command was initiated on the mobile app to the time that the device corresponding to the command actually acted) at three distances (2m, 5m, and 8m) was evaluated. For every command type (fan, LED, servo, buzzer) 15 operations were performed to guarantee validity. As shown in Figure 4, all commands executed in under 150 ms, meeting real-time control requirements for indoor smart office settings.

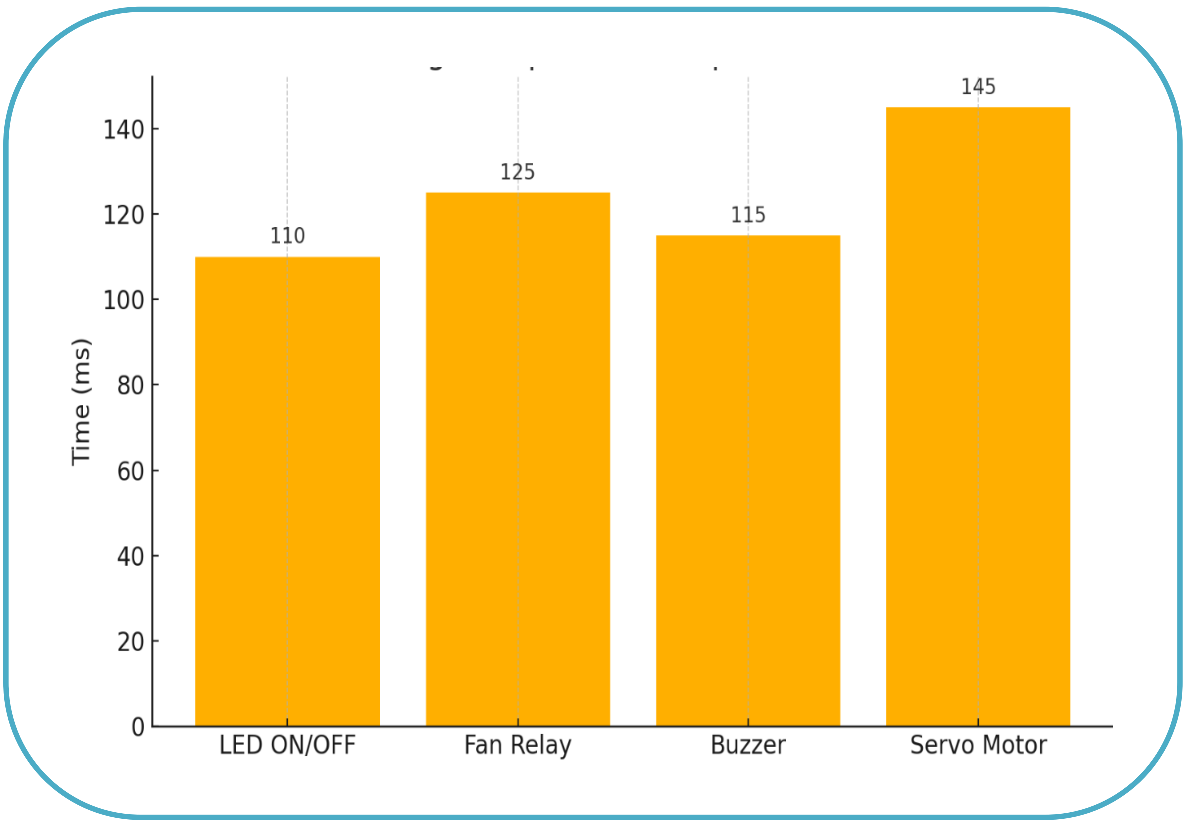


Figure 4. Response Time Evaluation

5.2 Bluetooth Signal Range Testing

The system was tested for signal reliability across increasing distances within an office mock-up. Signal strength was assessed based on command delivery failure rate and connection drop events. As shown in Figure 5, the system is reliable within 8 meters, ideal for single-room or adjacent-room deployments without range extenders.

ISSN: 3079-5354

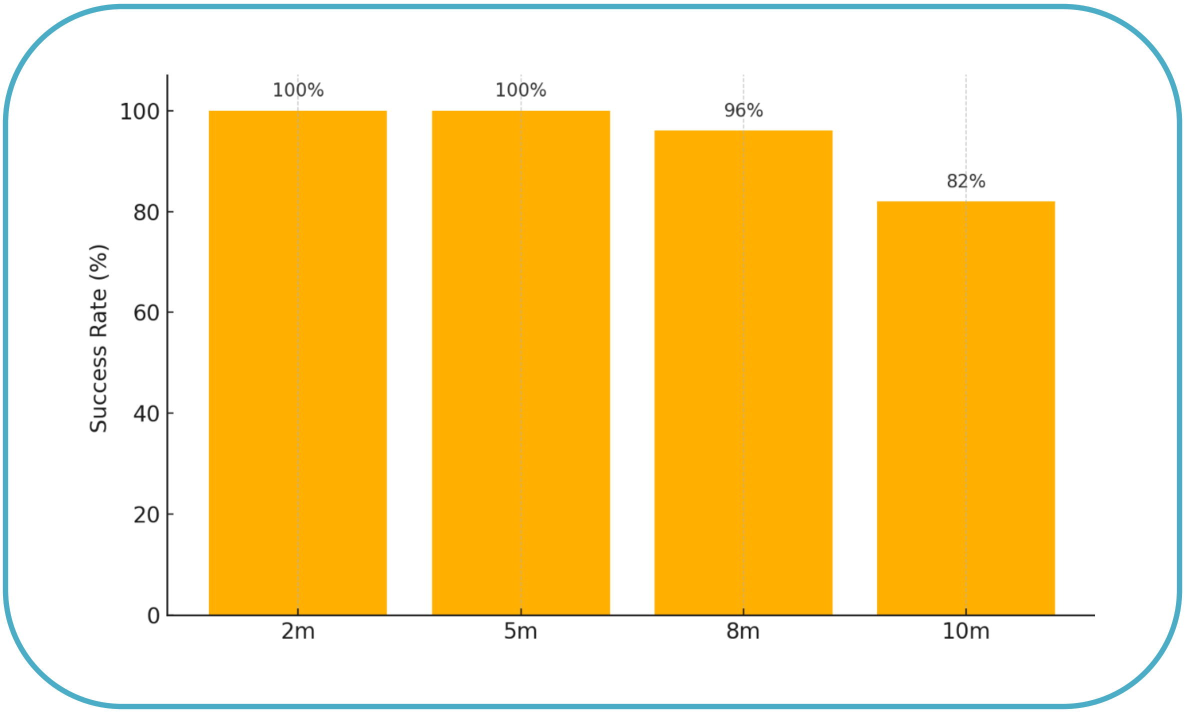


Figure 5. Bluetooth Signal Range Testing

5.3 Power Efficiency Analysis

Power consumption was measured under idle and active states of the ESP32 with connected modules. As shown in Figure 6, the system operates at very low power, supporting sustainable long-term operation even with UPS or battery support in environments with power instability.

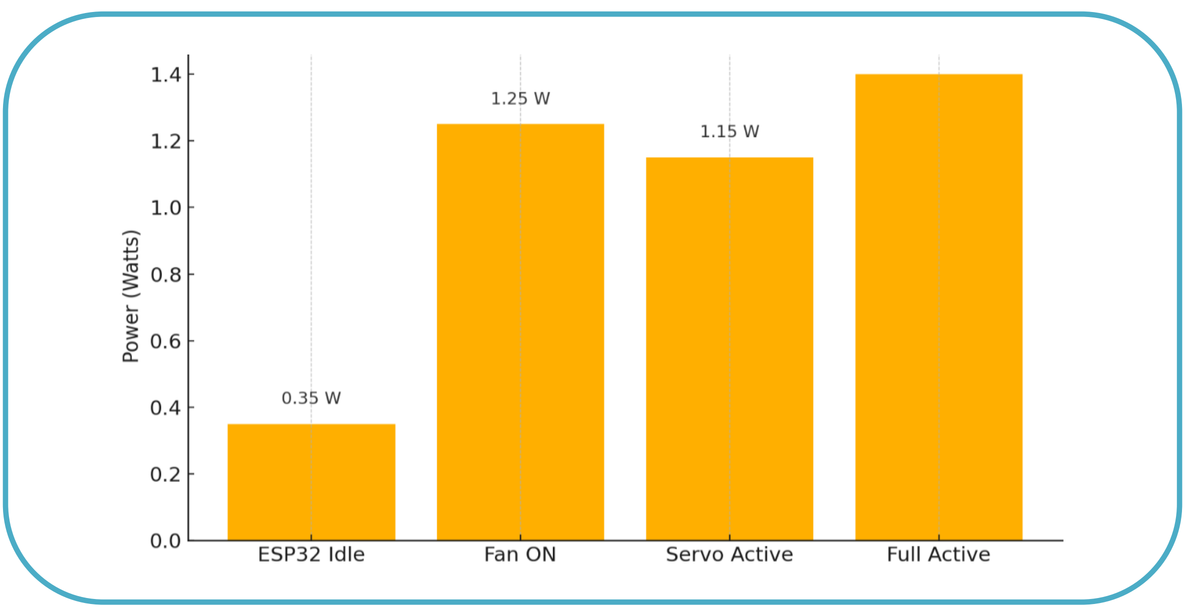


Figure 6. Power Efficiency Analysis

 ISSN: 3079-5354

5.4 Component Reliability and Robustness

All devices functioned normally over 200+ cycles of ON/OFF/rotate operations. As shown in Figure 7, the relay module showed no mechanical degradation, and the ESP32 maintained stability during all tests without overheating.

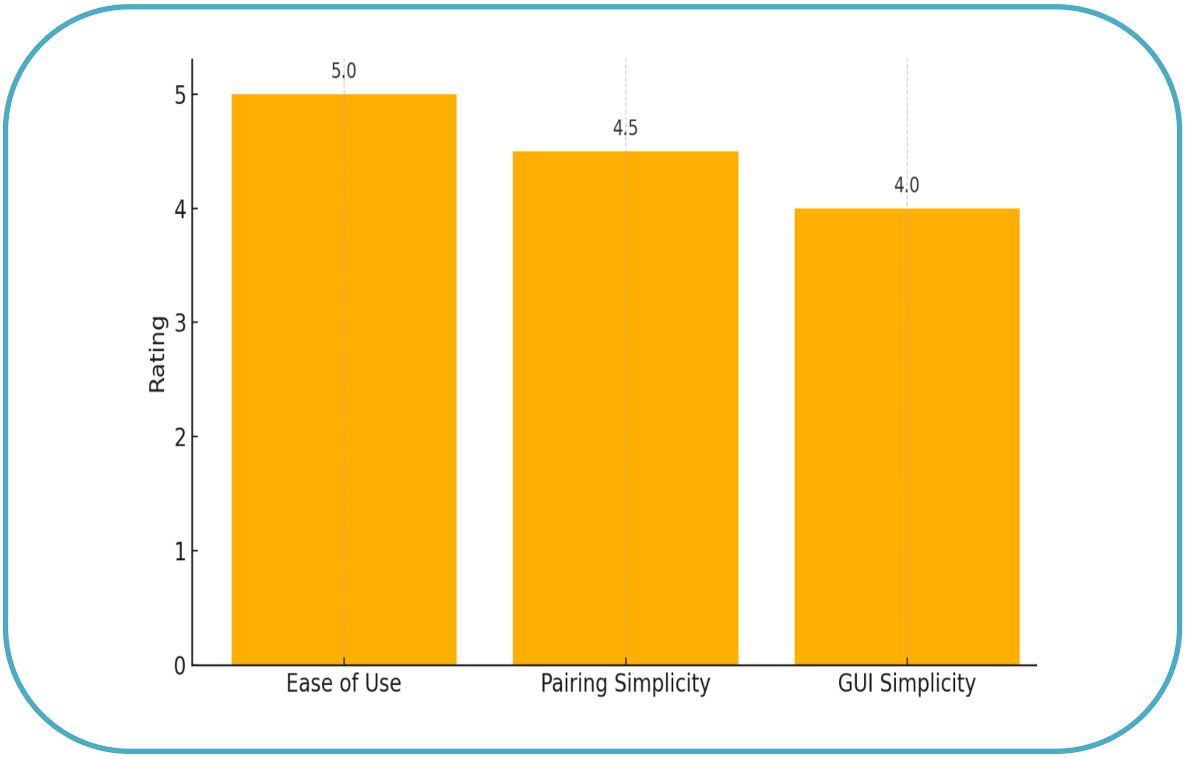


Figure 7. Component Reliability and Robustness

6. Discussion

This section begins with critical discussions on the design results, and then compares the proposed system with other works and provides the merits and disadvantages of the proposed system along with the future potential of real-life deployments.

6.1 Comparisons with Other Approaches

The proposed system effectively resolves the serious drawbacks of traditional smart automation systems: the dependency of internet, exposure to security threats, and overhead for deployment. Table 1 presents that with a cloud-based smart office con- figuration, there is significant flexibility, but at a price; for example, data leakages are possible, the cloud service has potential downtime, and a node can be controlled remotely without the owner's permission.

Table 1. Comparative Analysis of Smart Office Automation Systems

Feature	This Work (ESP32 + Blue-tooth)	Cloud-Based Systems	Wi-Fi Smart Switches

Offline Operation	Yes	No	Partial
Local Security (No	Yes 120–150 ms	No	Partial
Internet) Command	Planned (ESP- NOW, AES)	Variable	Around 200 ms
Latency Encryption	Yes	Yes (Cloud-side)	No
Supported	< $20		
		Moderate	Moderate
	Yes		
Mobile App		> $50	$30
Simplicity Cost		Partial	No
(USD)			
Modularity			

In contrast, this system is fully offline, communicates via Bluetooth, and enables dependable control with low latency (<150 ms). In contrast to Wi-Fi reliant solutions which need for a connection to be stable at all times and the routers must be correctly configured, ESP32 Bluetooth still remains simple and locally controllable and is suitable for applications in environments where security, privacy or infrastructure limitations are not allowing Wi-Fi-based systems to be easily employed.

6.2 Key Advantages

• Offline Security Superiority: When there is no dependence on cloud-based servers and other network resources, this HSIQRCAM technology is immune from spoofing, denial-of-service and credential exposure attacks. Security is also rounded out with hardware Bluetooth pairing and controls restricted to only trusted devices.

• High Performance and Cost Effective: The ESP32 processor and complementary components use ¡1.5W even at the maximum level of operation, making it reliable to be powered by simple power supply infrastructure or any back-up sources. The total hardware cost was less than 20, which was affordable for low-budget institutions or developing country settings.

• Scalable and modular: The architecture is modular in that the concept of adding additional relays, cluster centers, sensor (e.g., motion, temperature), or range extending components (e.g., relays) or even permission granting components (e.g., RFID or biometrics) that need not re-design the architecture from scratch. 9309461hayes

6.3 Limitations

There are several limitations in the present prototype that may affect its general practicality:

• Bluetooth signal will be weakened if beyond 8-10 meters indoor with obstacles. This limits it use to up to medium sized offices without BLE mesh or repeaters.

• Unencrypted Communication: Even though pairing limits accessibility, we currently

do not have command level encryption in the prototype. If some evil person does manage to establish a pairing, then they can also sniff your control codes. The next versions of this project will use AES or a secure messaging protocol like ESP-NOW.

• Lack of Manual Pairing: A manual pairing is necessary one time between the mobile

phone and ESP32. Even it’s very secure, that’s a little bit too much load on not- technical user.

• No App Feedback Mechanism: The app does not provide real-time status updates or feedback (e.g., “Fan is ON”), which may limit usability in rigging of greater complexity.

7. Conclusion and Future work

This paper described the design and implementation of a secure, smart, offline office automation system, where ESP32 microcontroller and Bluetooth communication was utilized. By comparison with traditional IoT platforms with cloud and/or Wi-Fi gate- ways, in this study we aimed to address local control, privacy, and cost – requirements relevant in cases of constrained internet connectivity and prioritization of security. The following proved to be successful: Dependable Bluetooth communication (average response time less than 150 ms). Work across an indoor range of up to 8 meters and is perfect for small to medium-sized offices. Affordable hardware (costing <20) and low power consumption. A modular smart home automation system that can control air fans, lights, buzzers and doors all through the mobile application. Moreover, the offline property of the system also improves security because it reduces its attack sur- face towards efficient, convenient and flexible user-side devices that do not have to rely on cloud services. A test usability was also carried out in a pilot which confirmed the accessibility and user friendliness of the solution.

Corresponding author

Mahmood A. Al-Shareeda
mahmood.alshareedah@stu.edu.iq

Acknowledgements
NA

Funding
NA

Contributions
M.A.A; A.N.J; M.T.H; M.S.F; Conceptualization, M.A.A; A.N.J; M.T.H; M.S.F; Investigation, M.A.A; A.N.J; M.T.H; M.S.F; Writing (Original Draft), M.A.A; A.N.J; M.T.H; M.S.F; and M.A.A; A.N.J; M.T.H; M.S.F; Writing (Review and Editing) Supervision, M.A.A; A.N.J; M.T.H; M.S.F; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

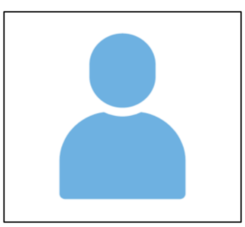
References

[1] Mu, X., & Antwi-Afari, M. F. (2024). The applications of Internet of Things (IoT) in industrial management: A science mapping review. *International Journal of Production Research, 62*(5), 1928–1952.
[2] Al-Mekhlafi, Z. G., Al-Janabi, H. D. K., Khalil, A., Al-Shareeda, M. A., Mohammed, B. A., Alsadhan, A. A., Alayba, A. M., Saleh, A. M. S., Al-Reshidi, H. A., & Almekhlafi, K. (2024). Lattice-based cryptography and fog computing-based efficient anonymous authentication scheme for 5G-assisted vehicular communications. *IEEE Access.*
[3] Nayab, Hussain, S., Alabrah, A., Ullah, S. S., Khattak, H., Alfakih, T. M., & Ullah, I. (2022). An efficient online/offline signcryption scheme for Internet of Things in smart home. *Wireless Communications and Mobile Computing*, *2022*(1), 4215441.
[4] Nassereddine, M., & Khang, A. (2024). Applications of Internet of Things (IoT) in smart cities. In *Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy* (pp. 109–136). CRC Press.
[5] Al-Shareeda, M. M. A., Anbar, M., Alazzawi, M. A., Manickam, S., & Hasbullah, I. H. (2020). Security schemes based conditional privacy-preserving in vehicular ad hoc networks. *Indonesian Journal of Electrical Engineering and Computer Science, 21*(1).
[6] Santhikiran, B., Nagaraju, L., Sattar, S. A., Chandra, D. B., & Jayasankar, Y. (2023). Design and implementation of smart home system based on IoT and ESPRainmaker. *International Transactions on Electrical Engineering and Computer Science, 2*(2), 70–79.
[7] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A holistic analysis of Internet of Things (IoT) security: Principles, practices, and new perspectives. *Future Internet, 16*(2), 40.

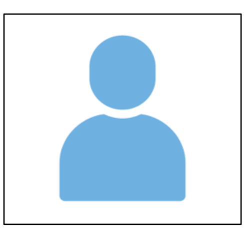
[8] Al-Shareeda, M. A., Anbar, M., Manickam, S., Hasbullah, I. H., Abdullah, N., Hamdi, M. M., & Al-Hiti, A. S. (2020). NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs). *Applied Mathematics, 14*(6), 1–10.
[9] Uzoka, A., Cadet, E., & Ojukwu, P. U. (2024). The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications. *Comprehensive Research and Reviews in Science and Technology, 2*(02), 055–073.
[10] Al-Shareeda, M. A., Manickam, S., Saare, M. A., & Arjuman, N. C. (2023). Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network. *Indonesian Journal of Electrical Engineering and Computer Science, 29*, 518–526.
[11] Mustofa, A. A., Dagnew, Y. A., Gantela, P., & Idrisi, M. J. (2023). SECHA: A smart energy-efficient and cost-effective home automation system for developing countries. *Journal of Computer Networks and Communications, 2023*(1), 8571506.
[12] Aghenta, L. O., & Iqbal, T. (2019). Design and implementation of a low-cost, open source IoT-based SCADA system using ESP32 with OLED, ThingsBoard and MQTT protocol. *IMS Electronics and Electrical Engineering, 4*(1), 57–86.
[13] Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2022). Intelligent drone-based IoT technology for smart agriculture system. In *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)* (pp. 41–45). IEEE.
[14] Irugalbandara, I. C., Naseem, A. S. M., Perera, M. S. H., & Logeeshan, V. (2022, June). HomeIO: Offline smart home automation system with automatic speech recognition and household power usage tracking. In *2022 IEEE World AI IoT Congress (AIIoT)* (pp. 571-577). IEEE.
[15] Irugalbandara, I. C., Naseem, A., Perera, M., & Logeeshan, V. (2022). HOMEIO: Offline smart home automation system with automatic speech recognition and household power usage tracking. In *2022 IEEE World AI IoT Congress (AIIoT)* (pp. 571–577). IEEE.
[16] Litayem, N. (2024). Scalable smart home management with ESP32-S3: A low-cost solution for accessible home automation. In *2024 International Conference on Computer and Applications (ICCA)* (pp. 1–7). IEEE.
[17] Jion, M. S. A., & Ahmad, M. (2024). A smart and secured office system using IoT. In *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)* (pp. 1–6). IEEE.

Biographies

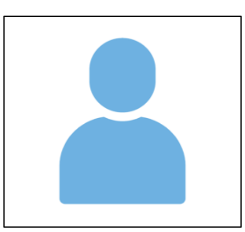
Dr. Mahmood A. Al-Shareeda received the B.S. degree in communication engineering from Iraq University College (IUC), the M.Sc. degree in information technology from Islamic University of Lebanon (IUL), in 2018, and the Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He was a Postdoctoral Fellowship with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He is currently an Assistant Professor of communication engineering with IUC. His current research interests include network monitoring, the Internet of Things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security. mahmood.alshareedah@stu.edu.iq



Ahmed Nader jafer Computer Technology Engineering, Iraq University College, Basra, Iraq



Mohammed Tahseen Hashem Computer Technology Engineering, Iraq University College, Basra, Iraq



Murtaza Salman Fajr Computer Technology Engineering, Iraq University College, Basra, Iraq