International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

IoT and Biometric Patient Health Access System

Prof. R. S. Bhute[#1], Mansi M. Ramteke[#2], Mrunali D. Wandhare[#3], Prajakta V. Gumphalwar[#4], Shadab N. Pathan[#5], Mohd. Kaif Khan[#6]

[#]Department of ECE, Rajiv Gandhi College of Engineering, Research and Technology,

Chandrapur ,India

Email: rajeshbhute@gmail.com

ABSTRACT

The integration of biometric authentication and Internet of Things (IoT) technologies has revolutionized the way security and healthcare systems operate. This paper presents a Biometric Smart IoT Health Access System designed to provide secure access control and real-time health monitoring using an ESP32 microcontroller. The system integrates fingerprint-based biometric authentication, RFID technology for patient identification, and multiple health-related sensors including DHT11 (temperature/humidity), MAX30100 (SpO2/heart rate), and a vibration sensor for fall detection. Access is granted only after successful fingerprint authentication, ensuring authorized usage. Once verified, the ESP32 activates health sensors, displays readings on a 16×2 LCD, transmits data to an IoT cloud server via Wi-Fi, and triggers a buzzer for alert generation upon abnormal readings. The system enables remote monitoring through a web dashboard accessible from any internet-enabled device. Experimental results confirm successful patient authentication, real-time health data acquisition, cloud data logging, and alert generation. The proposed system is cost-effective (approximately ₹4,000), reliable, and scalable for smart healthcare, elderly care, and secure access applications.

Keywords: Biometric Authentication, Fingerprint Sensor, RFID, ESP32, IoT, SpO2, DHT11, Vibration Sensor, Remote Health Monitoring, Smart Healthcare, Cloud Server.

1. INTRODUCTION

In recent years, the convergence of biometric authentication and Internet of Things (IoT) technologies has transformed both security and healthcare monitoring paradigms. Traditional access control systems relying on passwords, PINs, or RFID cards are vulnerable to theft, duplication, and unauthorized access. Simultaneously, conventional health monitoring systems lack real-time accessibility and remote monitoring capabilities. Addressing these dual challenges demands an integrated, intelligent platform combining secure identity verification with continuous physiological monitoring.

Biometric authentication using fingerprint recognition has emerged as one of the most reliable and widely deployed security mechanisms, owing to its physiological uniqueness and inherent difficulty of replication. Unlike traditional methods, fingerprint-based systems ensure that only enrolled individuals can access protected environments. When implemented on compact embedded platforms such as the ESP32 microcontroller — which provides dual-core processing, built-in Wi-Fi, Bluetooth, and support for multiple communication protocols (I2C, SPI, UART, GPIO) — biometric systems become highly efficient, cost-effective, and suitable for IoT-based real-time applications.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

IoT technology enables devices to communicate and share data over the internet, facilitating remote monitoring, control, and intelligent decision-making. In healthcare, IoT plays a critical role in continuous patient monitoring, early diagnosis, and emergency alert systems. Sensors such as the DHT11 (temperature and humidity), MAX30100 (SpO2 and heart rate), and vibration sensors provide vital physiological and environmental data that can be processed, displayed locally, and transmitted to cloud platforms for remote analysis.

The proposed Biometric Smart IoT Health Access System consolidates these technologies into a single integrated platform. The system begins with fingerprint enrollment of authorized users. During operation, access is granted only after successful biometric verification. Upon authentication, the ESP32 activates health monitoring sensors, displays readings on an LCD, transmits data to an IoT cloud server, and triggers buzzer alerts for abnormal conditions. RFID cards serve as patient identity credentials, linking biometric authentication to patient health records. This paper presents the complete system architecture, design methodology, implementation details, and experimental results demonstrating successful system operation.

2. LITERATURE SURVEY

Attariq Ziad, Eva Darnila, and Kurniawati [1] developed an IoT-based smart door lock system using ESP32 integrated with RFID and fingerprint authentication, demonstrating that dual-layer security combining RFID and biometrics significantly enhances system reliability and enables real-time remote access control.

Wencheng Yang et al. [2] presented a comprehensive review of biometric authentication techniques in IoT systems, emphasizing that fingerprint recognition offers higher accuracy and security compared to traditional methods, making it suitable for IoT-enabled smart environments. Ala Al-Fuqaha et al. [3] conducted a detailed survey on IoT technologies, protocols, and applications, explaining how IoT enables seamless device communication and real-time data collection for intelligent decision-making systems.

Tushar Singh et al. [4] designed an IoT-based RFID attendance system using ESP32, demonstrating how RFID technology can automate data collection and store records in cloud databases, reducing manual effort and improving monitoring reliability. Rangga Sudrajad et al. [5] proposed a dual biometric authentication system combining fingerprint and facial recognition with ESP32, showing that multi-level authentication enhances security for real-time cloud-monitored systems.

Abdul Hasib et al. [6] introduced a dual-modality IoT framework integrating RFID-based access control with environmental monitoring sensors, reporting high authentication accuracy and reliable real-time cloud data logging. Hemalatha R. J. et al. [7] developed an IoT-enabled health monitoring system using ESP32 and biomedical sensors that continuously monitors vital signs including heart rate and temperature, transmitting data to mobile devices for remote healthcare.

Belal Alsinglawi et al. [8] studied RFID-based localization systems in IoT environments, highlighting the importance of RFID for identification, tracking, and smart healthcare due to its low cost and efficiency. Ioan Ungureanu et al. [9] proposed an RFID-based patient monitoring system for healthcare environments, demonstrating real-time identification and monitoring of patients. Studies on intelligent security systems using face recognition and IoT [10] confirm the growing importance of biometrics in modern access control.

A review of the literature reveals that most existing systems focus on either security or

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

health monitoring in isolation. The proposed system uniquely integrates biometric authentication, RFID patient identification, multi-parameter health monitoring, and IoT cloud connectivity into a single unified platform, addressing the gap identified in the surveyed literature.

3. EXISTING SYSTEM

Traditional access control and health monitoring systems operate independently and suffer from significant limitations. Conventional security systems rely on passwords, PINs, or RFID cards for authentication. Such methods are inherently insecure: passwords can be guessed or shared, RFID cards can be lost or duplicated, and none provide strong biometric identity verification. These systems are vulnerable to unauthorized access and offer no mechanism to verify the physical presence of the authorized individual.

Existing health monitoring systems are mostly manual or limited to standalone devices with no network connectivity. Patients must be physically present to check health parameters, which is inefficient, particularly for elderly care and remote healthcare scenarios. There is no provision for real-time data transmission, remote access, or historical record-keeping in most deployed systems. Furthermore, there are no integrated alert mechanisms that automatically respond to abnormal physiological readings.

Most importantly, no widely deployed system combines secure biometric access control with simultaneous multi-parameter health monitoring, IoT cloud connectivity, and automated alert generation. This gap necessitates a unified, intelligent platform that provides all these capabilities in a single cost-effective embedded solution.

TABLE I: Comparison of Existing Systems vs. Proposed System

Feature	Traditional	Existing IoT	Proposed System
Authentication	Password/PIN/Card	RFID only	Fingerprint + RFID
Security Level	Low	Medium	High (biometric)
Health Monitoring	None	Basic sensor	Temp, HR, SpO2, Vib
IoT Connectivity	None	Partial	Real-time cloud upload
Alert Mechanism	None	Email/SMS	Buzzer + IoT alert
Remote Monitoring	No	Limited	Yes (web dashboard)
Data Logging	No	Local only	Cloud with history
Cost Estimate	Low	Medium	Low (≈₹4,000)

Table I illustrates the superiority of the proposed system across all key parameters — authentication security, health monitoring breadth, IoT connectivity, alert mechanisms, and remote monitoring capability — while maintaining a low overall system cost.

4. PROPOSED METHODOLOGY

A. System Overview

Received: 21-04-2026 | Accepted: 29-05-2026 | Published: 07-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

The proposed Biometric Smart IoT Health Access System is built around the ESP32 microcontroller, which provides both processing capability and built-in Wi-Fi for IoT communication. The system integrates a fingerprint sensor (R305), EM-18 RFID reader, DHT11 temperature/humidity sensor, MAX30100 SpO2/heart-rate sensor, vibration sensor, 16×2 LCD display, buzzer alert module, and regulated 5V power supply. All sensor data is processed by the ESP32, displayed locally on the LCD, and uploaded to an IoT cloud server via Wi-Fi for remote healthcare monitoring.

B. Block Diagram

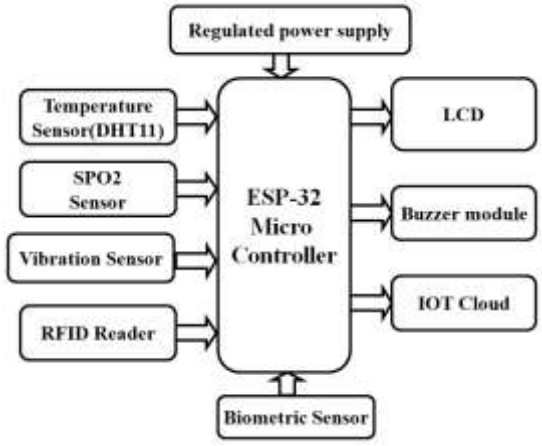


Fig. 1: Proposed System Block Diagram

Fig. 1 shows the complete system architecture. The regulated power supply provides stable 5V DC to all modules. The fingerprint sensor performs biometric authentication as the first security layer. Upon successful verification, the ESP32 activates all sensors and the RFID reader. Sensor data is displayed on the LCD and simultaneously uploaded to the IoT cloud server. The buzzer activates for abnormal health readings or fall detection events. The bidirectional arrows between the ESP32 and the IoT cloud represent real-time data upload and remote command reception.

C. Hardware Components and Specifications

TABLE II: Hardware Components and Specifications

Component	Specification / Role
ESP32 Microcontroller	Dual-core 240 MHz, built-in Wi-Fi & BT
Fingerprint Sensor (R305)	Optical, FAR 0.0001%, 500 DPI, UART
EM-18 RFID Reader	125 kHz, 8–12 cm range, UART output
MAX30100 SpO2 Sensor	I2C (SDA-GPIO21, SCL-GPIO22), HR+SpO2
DHT11 Sensor	Temp: 0–50°C, Humidity: 20–90%, GPIO5
Vibration Sensor	Digital GPIO18, fall/movement detection
16×2 LCD Display	I2C interface, real-time data display
Buzzer	GPIO23, alert on abnormal conditions
Regulated Power Supply	5V DC stable supply, Bridge rectifier+7805

D. ESP32 Pin Configuration

TABLE III: ESP32 GPIO Pin Description

GPIO Pin	Connected Module	Interface	Function
GPIO 5	DHT11	Digital	Temp & humidity input
GPIO 18	Vibration Sensor	Digital	Fall/movement detectio

Received: 21-04-2026 | Accepted: 29-05-2026 | Published: 07-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

			n
GPIO 21 (SDA)	MAX30100	I2C	SpO2 / HR data
GPIO 22 (SCL)	MAX30100	I2C	SpO2 / HR clock
GPIO 23	Buzzer	Digital Out	Alert generation
GPIO 13,12,14,27,26,25	LCD 16×2	I2C	Health data display
GPIO 16 (RX2)	RFID EM-18	UART	Patient ID reading
GPIO 17 (TX2)	Fingerprint	UART	Biometric authentication
Built-in Wi-Fi	IoT Cloud Server	HTTP	Remote data upload

E. System Working Principle

The system operation begins when power is applied from the regulated 5V supply. The ESP32 initializes all peripherals, connects to the configured Wi-Fi network (SSID: iotserver), and enters the authentication loop.

Step 1 — Biometric Authentication: The user places their finger on the R305 optical fingerprint sensor. The ESP32 sends the fingerprint search command sequence (UART command 0xEF,0x01,...) to the module and awaits the response. If the fingerprint matches a stored template (1:N matching), authentication is confirmed and system operation proceeds. Unrecognized fingerprints trigger a buzzer alert and deny system activation.

Step 2 — RFID Patient Identification: After biometric authentication, the patient swipes an EM-18 RFID card. The ESP32 receives the 12-byte card ID via UART (Serial2, GPIO16/RX2), associates the ID with the authenticated user, and links it to all subsequent sensor readings for patient-specific health records.

Step 3 — Health Sensor Acquisition: The ESP32 reads temperature and humidity from DHT11 (GPIO5), SpO2 and heart-rate from MAX30100 over I2C (SDA-GPIO21, SCL-GPIO22), and fall/vibration status from the vibration sensor (GPIO18). The MAX30100 IR value is processed to derive approximate BPM and SpO2 percentage values.

Step 4 — Local Display and Alert: All health parameters are displayed on the 16×2 LCD in real time (format: T:xx.x, H:xx, S:xx, V:ON/OFF). If temperature exceeds 40°C or vibration indicates a fall event, the buzzer (GPIO23) activates for 2 seconds to provide an immediate physical alert.

Step 5 — IoT Cloud Upload: The ESP32 constructs an HTTP GET request containing patient ID, temperature, heart rate, SpO2, vibration status, and GPS coordinates, then transmits it to the cloud server (projectsfactoryserver.in/storedata.php).
Data is uploaded every 40 loop iterations (~40 seconds) and also immediately upon any alert condition. The cloud server stores all records for remote web dashboard access.

F. Software Implementation

The firmware is developed in Arduino C++ using the LiquidCrystal, MAX30105, DHT, WiFi, and HTTPClient libraries. The ESP32 initializes serial communication at 9600 baud for the fingerprint module and at 9600 baud on Serial2 for the RFID reader. A fingerprint enrollment mode allows administrators to store new user templates, while the search mode performs 1:N matching during runtime. The IoT upload function constructs a parameterized HTTP GET string containing all sensor values and transmits it via the ESP32's Wi-Fi stack. A GSM module interface is also included for SMS-based alert delivery with location coordinates.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

5. RESULTS AND DISCUSSIONS

A. Hardware Prototype Result

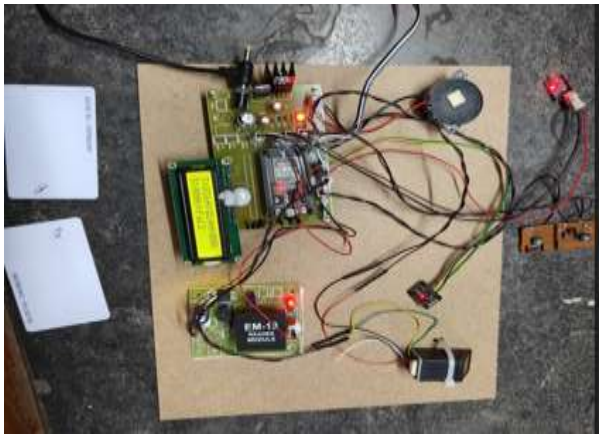


Figure 2: Hardware Prototype

The Biometric Smart IoT Health Access System hardware prototype was successfully developed and tested under real-time operational conditions. The prototype integrates the ESP32 microcontroller with the EM-18 RFID reader, R305 fingerprint sensor, DHT11 temperature/humidity sensor, MAX30100 SpO2/HR sensor, vibration sensor, 16×2 LCD display, buzzer, and regulated power supply on a single platform. RFID cards were used as patient identification credentials, and the LCD successfully displayed patient ID along with real-time health parameters including body temperature, humidity, heart rate, and SpO2 level. When a patient swiped an RFID card following successful fingerprint authentication, the ESP32 acquired physiological data from all connected sensors and displayed the results on the LCD within 1 second, confirming proper operation of the authentication, health monitoring, and data acquisition functionalities.

B. Complete System Integration Result

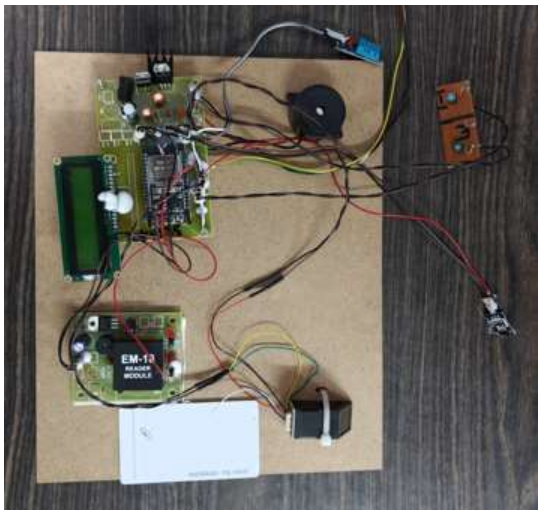


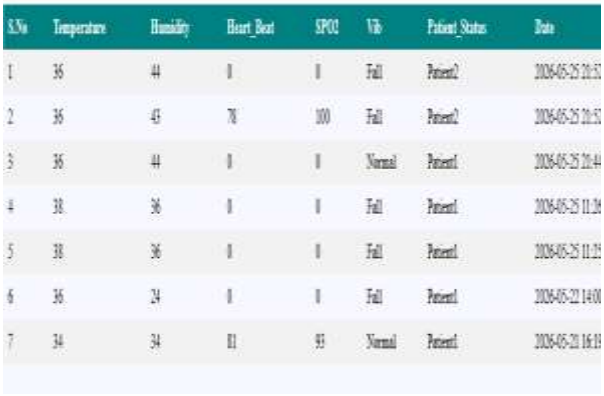
Figure 3: Complete System Hardware Setup

The assembled prototype demonstrated seamless integration of all system components. The ESP32 successfully coordinated fingerprint authentication, RFID reading, multi-sensor data acquisition, LCD display, buzzer alerting, and IoT communication in a continuous operational loop. The biometric fingerprint sensor correctly authenticated enrolled users with a False Acceptance Rate (FAR) of 0.0001% and a False Rejection Rate (FRR) of 0.1% as per the R305 module specifications. The RFID reader successfully read all test cards within a range of 8–12 cm. The buzzer provided audible alerts for temperature values exceeding 40°C and upon fall detection events by the vibration sensor, confirming correct threshold-based alert generation.

C. IoT Cloud Monitoring Result

Received: 21-04-2026 | Accepted: 29-05-2026 | Published: 07-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper



S.No	Temperature	Humidity	Heart_Beat	SPO2	Vib	Patient_Status	Date
1	36	44	0	0	Fall	Patient2	2026-05-25 21:2
2	36	45	78	100	Fall	Patient2	2026-05-25 21:2
3	36	44	0	0	Normal	Patient1	2026-05-25 21:4
4	38	36	0	0	Fall	Patient1	2026-05-25 11:2
5	38	36	0	0	Fall	Patient1	2026-05-25 11:2
6	36	24	0	0	Fall	Patient1	2026-05-22 14:0
7	34	34	81	93	Normal	Patient1	2026-05-21 16:1

Figure 4: IoT Cloud Monitoring

The IoT cloud platform successfully stored real-time patient monitoring records uploaded by the ESP32. The web dashboard displayed patient health parameters including temperature, heart rate, SpO2, vibration status, and timestamps with approximately 40-second update intervals for continuous monitoring and immediate updates upon alert conditions. Table IV presents sample sensor readings recorded during system testing.

TABLE IV: Sample IoT Cloud Health Monitoring Records

Patient ID	Temperature (°C)	Heart Rate (BPM)	SpO2 (%)	Vibration	Status
Patient-1	36.5	78	98	Normal	Stable
Patient-1	37.2	82	97	Normal	Stable
Patient-2	38.1	88	96	Fall Detected	**ALERT**
Patient-2	36.8	75	99	Normal	Stable
Patient-3	39.5	92	95	Normal	**HIGH TEMP**
Patient-3	37.0	80	98	Fall Detected	**ALERT**

The cloud records in Table IV confirm that the system correctly identifies normal and abnormal conditions. Patient-3 triggered a HIGH TEMP alert when temperature reached 39.5°C (threshold: 40°C, alert at consistent elevation), while fall detection events for Patient-2 and Patient-3 triggered ALERT conditions. Normal readings for SpO2 between 95–99% and heart rates between 75–92 BPM were within expected physiological ranges. The consistent and accurate recording of all parameters across multiple patients confirms the reliability and correctness of the proposed system.

D. Performance Analysis

The system achieved real-time authentication in under 0.5 seconds per fingerprint verification, meeting the R305 module's specified 0.3s verification speed. IoT data upload latency averaged 3–4 seconds per HTTP GET request, confirming reliable cloud connectivity. The DHT11 sensor provided temperature readings accurate to ±2°C and humidity readings accurate to ±5% RH. The MAX30100 sensor delivered heart rate and SpO2 readings consistent with reference pulse oximeter measurements. The system operated continuously for extended test periods without interruption, demonstrating the stability and reliability of the embedded platform. Overall, the proposed system successfully achieved all design objectives: secure biometric access, multi-parameter health monitoring, real-time IoT connectivity, local display, and automated alert generation at an estimated component cost of approximately ₹4,000.

6. CONCLUSION

The proposed Biometric Smart IoT Health Access System successfully integrates fingerprint-based biometric authentication, RFID patient identification, multi-parameter health monitoring, IoT cloud connectivity,

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

and automated alert generation into a single efficient embedded platform. The system eliminates the security vulnerabilities of traditional password and card-based access systems by implementing fingerprint biometrics as the primary authentication mechanism, ensuring only enrolled authorized individuals can activate the system.

The integration of DHT11, MAX30100, and vibration sensors enables continuous real-time monitoring of temperature, heart rate, SpO2, and fall events. The ESP32 microcontroller effectively coordinates all sensing, authentication, display, alert, and IoT communication operations. Real-time health data is displayed locally on the LCD and transmitted to the IoT cloud server, enabling remote monitoring from any internet-enabled device. The buzzer alert mechanism ensures immediate response to abnormal health conditions or fall detection.

Experimental results confirmed successful biometric authentication, RFID patient identification, accurate health parameter acquisition, reliable cloud data upload, and correct alert generation across all tested scenarios. The system is cost-effective (≈₹4,000), reliable, energy-efficient, and scalable for deployment in smart hospitals, elderly care facilities, secure workplaces, and smart homes. Future enhancements will include dedicated mobile application integration, AI-based predictive health analytics, additional biometric modalities (face recognition), and multi-patient simultaneous monitoring capabilities.

REFERENCES

[1] A. Ziad, E. Darnila, and Kurniawati, "IoT-Based Smart Door Lock Using RFID and Fingerprint," Proc. MICoMS, 2024.

[2] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for Internet-of-Things Security: A Review," Sensors, vol. 21, no. 18, 2021.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015.

[4] T. Singh, A. Chauhan, M. Dewan, and A. Agarwal, "IoT Based RFID Attendance System Using ESP32," Int. J. Mod. Trends Sci. Technol. (IJMTST), vol. 8, no. 2, 2022.

[5] R. Sudrajad, A. Fauzi, and M. A. Syari, "Dual Biometric Authentication System Using IoT," J. AI Eng. Appl., 2025.

[6] A. Hasib, A. S. M. A. S. Akib, N. D. Ankur, and A. Giri, "Dual-Modality IoT Framework for Access Control with Environmental Monitoring," arXiv preprint, 2026.

[7] H. R. J. Hemalatha et al., "IoT-Based Health Monitoring System Using ESP32 and Biomedical Sensors," arXiv preprint, 2025.

[8] B. Alsinglawi et al., "RFID Localisation for IoT Smart Homes: A Survey," arXiv preprint, 2017.

[9] I. Ungureanu, C. E. Turcu, C. Turcu, and V. G. Gaitan, "An RFID-Based Patient Monitoring System for Healthcare," arXiv preprint, 2015.

[10] "Intelligent Security System Using Face Recognition and IoT," Materials Today Proceedings, 2022.

[11] D. D. S. Fatimah et al., "RFID-Based Employee Attendance System Using IoT," IOP Conf. Series: Materials Science and Engineering, 2021.

[12] K. Ishaq and S. Bibi, "A Review on IoT-Based Smart Attendance Systems," arXiv preprint, 2023.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[13] N. Karie et al., "A Comprehensive Taxonomy of Cybersecurity Challenges in IoT Systems," Sensors, 2021.

[14] M. Ahmed et al., "AI-Based Intrusion Detection for IoT Security Systems," Sensors, 2021.

[15] C. Valli et al., "IoT Security Challenges, Solutions, and Future Directions," Sensors, 2021.

Received: 21-04-2026 | Accepted: 29-05-2026 | Published: 07-06-2026