International Journal of Cybersecurity Engineering and Innovation

ARTICLE INFO

Article History: Received: 24-01-2026, Revised: 20-04-2026, Accepted: 12-06-2026, Published: 15-06-2026
Corresponding author Email: *mahmood.alshareedah@stu.edu.iq*

This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).
Published by ITAP Publisher.

Vol. 2026 No.1

A Secure and Scalable IoT Home Automation Architecture with Web and Biometric Control

Alaa Ibrahim[1], Abbas Fadhil Kadhim[1], Abdulwahhab Essa Hamzah[1], Mahmood A. Al-Shareeda[2,3*]

[1]*Department of Communications Engineering, Iraq University College, Basrah, Iraq.*

[2] *Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq.*

[3] *College of Engineering, Al-Ayen University, Thi-Qar, 64001, Iraq.*

**Corresponding author(s). E-mail(s): mahmood.alshareedah@stu.edu.iq*

Abstract

The flourishing of the Internet of Things (IoT) is further driving smart home technology, facilitating remote supervision and automatic control over home appliances. Existing home automation systems are often insecure, not scalable, and lack integrated ways to control these applications. This paper presents a secure and scalable IoT-enabled home automation architecture that combines web control with face recognition biometrics to ensure system security and user friendliness. The developed system works with a Raspberry Pi acting as a cen- tral unit and is connected to IoT-based sensors, relay-based actuators, and a camera module. An authorized user is allowed to control home appliances at a distance by a browser-based interface, and Face is used to retrieve the identity of the user for authentication in it using OpenCV GUI, OpenCV image processing, and dlib. HTTPS with SSL/TLS and role-based access control are used to ensure secure communication. We extensively test the system using experiments in the real world, under which we show reliable device control, responsive interaction through the web, and efficient biometric authentication. The findings validate that the proposed design provides a viable, inexpensive, and privacy-preserving practical solution for secure smart home automation.

Keywords: Internet of Things (IoT), Smart Home Automation, Raspberry Pi, Biometric Face Recognition, Web-Based Control, Secure Communication, Access Control.

1. Introduction

The fast development of the Internet of Things (IoT) has significantly changed traditional homes and rendered them an intelligent smart home, enabling automated control, remote monitoring, and real-time control [1, 2]. IoT, by connecting sensors, actuators, and embedded devices via networked infrastructures, allows end-users to remotely operate home appliances efficiently and conveniently from distant places [3, 4]. With the boom of smart homes, secure, accessible communication and scalability of system design have become an essential research issue [5, 6].

Conventional home automation systems generally depend on mobile device applications, PIN-based authentication, or cloud-based services [7, 8]. These solutions only provide the very basics of automation but are often plagued by

security holes, small scalability, privacy worries, and disjointed user interfaces. Unauthenticated access, stolen credentials, and insecure communication pathways are all issues you would like to guard against, especially when remote connections are allowed [9, 10]. Therefore, the middleware for smart homes should include strong user authentication schemes and secure communication protocols [11, 12].

Biometric authentication is identified as a potential method to improve access security in IoT environments [13–15]. Face recognition, among biometric modalities, provides a non-invasive and user-friendly mode of identification without physical con- tact or the need for wearable hardware [16, 17]. Advancements in computer vision and embedded processing now enable running face recognition algorithms on low- cost embedded platforms. Nevertheless, how to incorporate biometric authentication mechanisms in IoT-based home automation solutions, noting proximity and being always connected in real time for privacy preserving and scalability, becomes an open question [18, 19].

Motivation Recent work has investigated the notion of using low-cost embedded platforms like Raspberry Pi for smart home automation, as they are cost-effective, flexible, and supported by a large community [20–22]. Raspberry Pi-based solutions can process sensor data and control logic locally without the need for cloud services, which results in the ability to increase user privacy [23, 24]. However, numerous implementations tend to emphasize device automation while omitting robust security solutions that encompass biometric authentication, secured communication, and access control in an integrated approach [25, 26].

Based on these issues, this paper suggests a secure and scalable IoT home automation architecture using web/browser/biometric control. The system consists of a combination of a control unit on Raspberry Pi, a web-based user interface to man- age remote devices, and finally, the biometric face recognition module used for secure access control. Communication is secure using HTTPS with SSL/TLS encryption, and use of the system is authorized for role-based access. Biometric processing is completely done locally at the edge, and it eliminates the latency and protects user privacy. The main contributions of this paper are highlighted as follows:

- We design a secure and scalable IoT-based home automation architecture centered on a Raspberry Pi that supports real-time device monitoring and control.
- We incorporate a web-based control interface allowing remote and encrypted con-trolled device access, networked node screen settings, appliance configuration, and monitoring.
- We implement a biometric face recognition–based access control module using OpenCV and dlib to enhance system security without relying on physical keys or passwords
- We implement secure communication and access control methods such as HTTPS with SSL/TLS encryption and role-based access control.
- We verify our system with experimental data in practice, and the results show that it is reliable, responsive, and robust to be used in biometric security.

The rest of this paper is structured as follows. Section 2 reviews the related work in IoT-based home automation and biometric access control. The proposed system architecture is then presented in Section 3. The methodology and implementation details are described in Section 4. Section 5 Experimental results and performance evaluation are presented. Section 6 discusses future work and open problems, and Section 7 gives concluding remarks.

2. Related Work

With recent developments in the Internet of Things (IoT), there has been a surge in research on smart home automation, which enables monitoring and control by users from anywhere on an increasing range of devices. Ghadekar et al. [27] introduced the smart home by amalgamating Iris-based bio- metric authentication and FisherFace-based emotion recognition. The system verifies the residents with their distinct iris features and modifies the home environment for resultant face emotions in real-time, which achieves good performance on both security and emotion-aware automation. Garg et al. [28] discussed secure access control in IoT-based smart homes with the deficiencies of conventional authentication schemes. The study demonstrates the capability of machine learning techniques for adaptation to real-time abnormality detection in dynamic and heterogeneous IoT systems, as well as decision-making. Yar et al. [29] suggested a smart home automation system with Internet-of-Things (IoT) and edge-computing that uses a resource-bound Raspberry Pi as the main controller. The approach is a system that combines automation, security, robustness, and energy conservation in the sense that it has shorter latency time (faster response),

lower bandwidth, and computation cost in comparison with other existing schemes. An energy-efficient smart house security system with a fingerprint door image acquisition device for automatic recognition is proposed by Devanathan et al. [30]. As a Raspberry Pi-based platform, the system provides secure, user-centric appliance control through web and mobile applications, implements room-level access control, and brings added energy savings by means of identity-based automation. A scalable client–server–based lamp control and monitoring system on wireless networks is pro- posed by Jagtap et al. [31]. The developed solution combines smart presence sensing and fine-grained usage analytics, empowering flexible lamp control and real-time monitoring as well as efficient operation, towards the realization of intelligent-by-design connected lighting systems for human-centric living spaces.

Notwithstanding such improvements, current systems are typically devoid of a cohesive architecture supporting integration of IoT automation, web-based remote control, biometric authentication, and secured communication as part of an interoperable platform. Existing systems can only tackle such elements independently and in a fragmented way, therefore preventing the actual deployment of any solution to real-world scenarios. Unlike that, this work proposes an IoT-based home automation architecture that is secure and scalable, integrating web-based control with face recognition using biometrics on a Raspberry Pi. Through locally implemented edge-level biometric processing and enhancement of secure communication by https, along with role-based access control, it attempts to overcome the limitations in existing approaches from security, privacy, and system integration perspectives.

3. Proposed System Architecture

The proposed system is an Internet of Things IoT enabled smart home automation architecture that utilizes web-based remote control in addition to biometric face recognition, leading to improved usability and security. Architecture The system follows a centralized model, in which the Raspberry Pi plays the role of hub and processor, responsible for interacting with software services, hardware components, and user interactions.

As shown in Figure 1, the network's framework consists of five major layers: Sensing and Actuation Layer; Processing and Control Layer; Biometric Authentication Layer; Web-Based Control Layer; and Security and Communication Layer. This layered approach delivers modularity, scalability, and ease in bringing in more devices or services.

- Processing and Control Layer: At the heart of the device is a Raspberry Pi 4 acting as the controller. It collects sensor information, triggers automation logic, authenticates biometrically, and controls attached actuators. It communicates with add-on devices via GPIO pins and even has built in Wi Fi & Bluetooh. Python is the main programming language, allowing easy access to hardware control, web services, and computer vision libraries. With the centralized processing model, system management becomes easy, and real-time decisions can be made.

- Sensing and Actuation Layer: This layer includes multiple IoT sensors and actuators connected in the smart home context. Typical components include: Environmental sensors (such as temperature and humidity sensors); Motion detection sensors; Camera module for face recognition; and Relay board to switch-on/off domestic appliances: lights, fans, door locks, etc. Relay modules serve as a mechanism that allows the output signals from the Raspberry Pi to activate high-voltage appliances without safety concerns. Such a layer makes it possible to act and interact directly with the real world.

- Biometric Authentication Layer: In order to increase the security of the system, a facial recognition module as a biometric authentication module is embedded in the architecture. A camera connected by cable to the Raspberry Pi captures the user's face and tries to guide it. We adopt OpenCV and dlib to implement a face recognition system and perform the tasks of face detection, feature extraction, and identity verification. Face features of the authorized users are securely preserved inside the local database. If successful, the right relay will be activated to grant the user access, e.g., unlock the door, and enable system control. This biometric stratum eliminates dependence on the physical key or access card and makes it much safer from unauthorized entry.

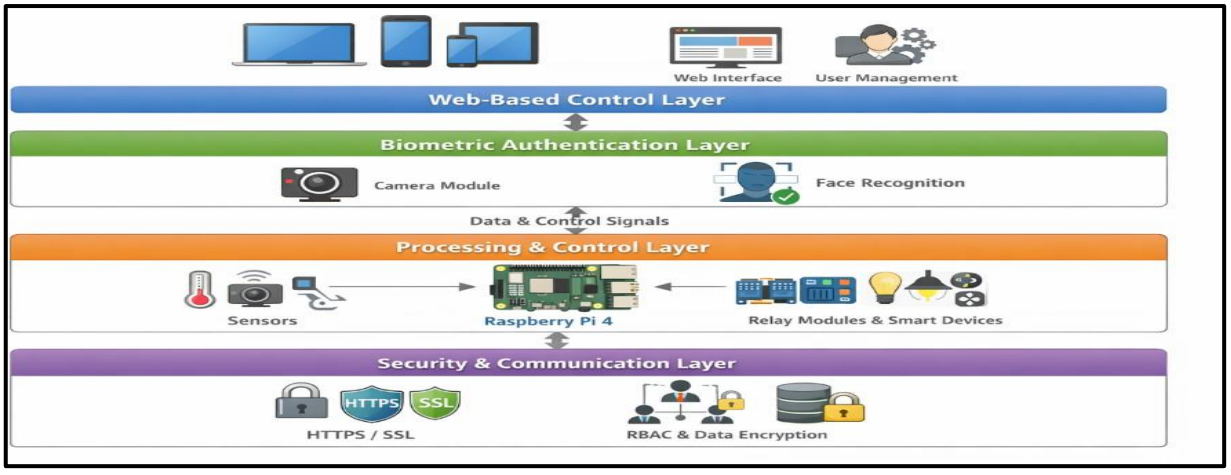


Figure 1. Architecture of the proposed IoT-based home automation system with web and biometric control.

- Web-Based Control Layer: The control layer, via a web page, enables users to remotely monitor and control home appliances in a unified manner through a simple user interface. You can access it from anywhere on an internet-enabled device, including mobile devices, laptops, and desktops. The web application is run directly off the Raspberry Pi with a slim-web framework. It enables users to: Turn appliances on or off; Check their status in real time; Manage user access and permissions; and View access and system logs. Real-time updates are provided that make it easy to use scripts, even directly hosted on GitHub through asynchronous communication techniques such as AJAX or WebSockets to provide a fast and responsive user experience.

- Security and Communication Layer: Security is a cornerstone within the proposed architecture. Data communication between the web interface and Raspberry Pi is encrypted with SSL/TLS over HTTPS to guarantee the privacy, authenticity, and integrity of data. Authorization methods such as username–password login and role- based access control (RBAC) are enforced to limit the access of systems according to user entitlements. In addition, the sensitive data, such as biometrics and system logs, is protected to avoid unauthorized exposure. This layer guarantees the security of the system against usual cyber threats like unauthorized operation, data reading, and man-in-the-middle attacks.

4. Methodology and Implementation

In this section, we discuss the methods used for designing, developing, and evaluating the proposed secure and affordable IoT home automation system. The Kushep-Vision Program is implemented in a layered and modular manner that provides flexibility, reliability, and expandability capabilities. Hardware and software are combined to realize a web-based control and biometric authentication in a homogeneous system. Figure 2 shows the hardware configuration of the proposed system, illustrating the integration of the Raspberry Pi, camera module for biometric authentication, relay- based actuation, and IoT sensors.

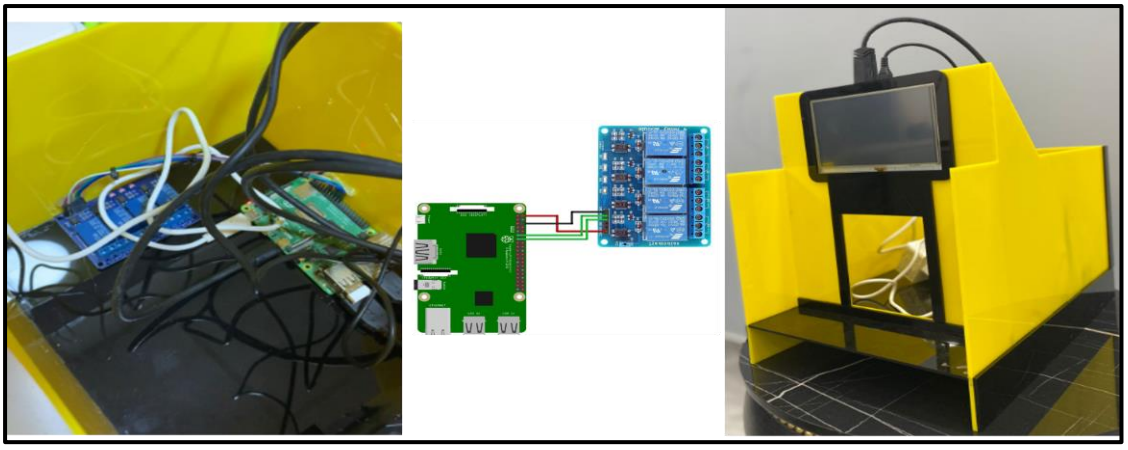


Figure 2. Physical hardware setup and wiring of the proposed IoT home automation system using Raspberry Pi and relay modules.

• Raspberry Pi-based Central Control Unit: The Raspberry Pi 4 acts as the brain and hub of the designed system. It acts as an automation controller, the bridge between layers of a system, manages communications and processes biometric data and device actions. The Raspberry Pi is powerful to perform real-time face recognition and process web server/GPIO instructions at the same time. It is equipped with a Wi-Fi integrated interface that supports remote access and real-time monitoring of the system.

• Camera Module: The Raspberry Pi is provided with a camera module for bio- metric face recognition authentication. The camera is constantly taking pictures as long as there's a picture being taken, then it sends these image frames to the processor for processing. The chosen camera gives enough resolution and image frequency for a perfect face identification and recognition in the average indoor lighting environment.

• Sensors and Actuators: Integrate with several IoT sensors to sense environmental conditions and system events. Example sensors are motion detectors and environmental sensors that support contextual information for control actions. Relay modules are used for actuation, which ensures that the Raspberry Pi can handle high-voltage household devices like lighting systems, fans, or electronic door locks. The relay module serves as an electrically-isolated switch, ensuring the safety of the low-voltage control part.

• Relay Module Configuration: They attach to the Raspberry Pi GPIO and are switched on or off in response to software commands. There is one relay channel for each appliance or actuator. When an accepted control command or positive bio- metric authentication is received, the Raspberry Pi sets the pin to high and closes (or opens) the relay to turn on (or off) the device to be controlled. In this way, the effective and fault-proof control of home devices is guaranteed.

• Power Supply and Wiring: The Raspberry Pi and other peripheral devices are powered by a stable power supply to ensure the continuity of work. Good wiring methods are used to help limit signal contamination, and inadvertent unplugging may also be avoided. The control and load lines are electrically separated by the relay modules; control and load isolation is integrated into the system, which improves safety and reliability. All connections are tidied and fixed to ensure maintenance and expand trouble-free.

Joining the Raspberry Pi, camera unit, sensors, and relay-based actuators together creates a single hardware platform that can be used to support secure IoT home automation applications. The modular hardware architecture makes it easy to expand and add new sensors and devices without significantly changing the design. This hard- ware layout is a robust support for the software-level automation and biometric access control capabilities described in the proposed work.

4.1 Software Implementation

This software realization of the proposed framework should enable reliable device control, secure communication, and efficient biometric authentication in a cohesive IoT infrastructure, as shown in Figure 3. The software stack is implemented on the Raspberry Pi and structured in a modular way to support scalability, maintainability, and real-time operation.

• OS and development environment: The Raspberry Pi is based on the Raspberry Pi OS, a Linux distribution running an optimized version of the Linux kernel that has been customized to run as an embedded operating system. It has strong support for hardware interfacing, networking, and multitasking. Here, the software part is written, and everything that will be running in it, i.e., the programs we'll write, will run at a lower level to provide stability due to hardware.

• Control and Automation Layer: The control system and automation logic is developed with the Python programming language due to its rich library ecosystem and compatibility with GPIO interfaces. Sensor data acquisition, relay activation, and state transition of the system are controlled by python scripts. It reduces user commands from the web interface into actions which are then executed in real time, guaranteeing low-latency response and enable to work robustly.

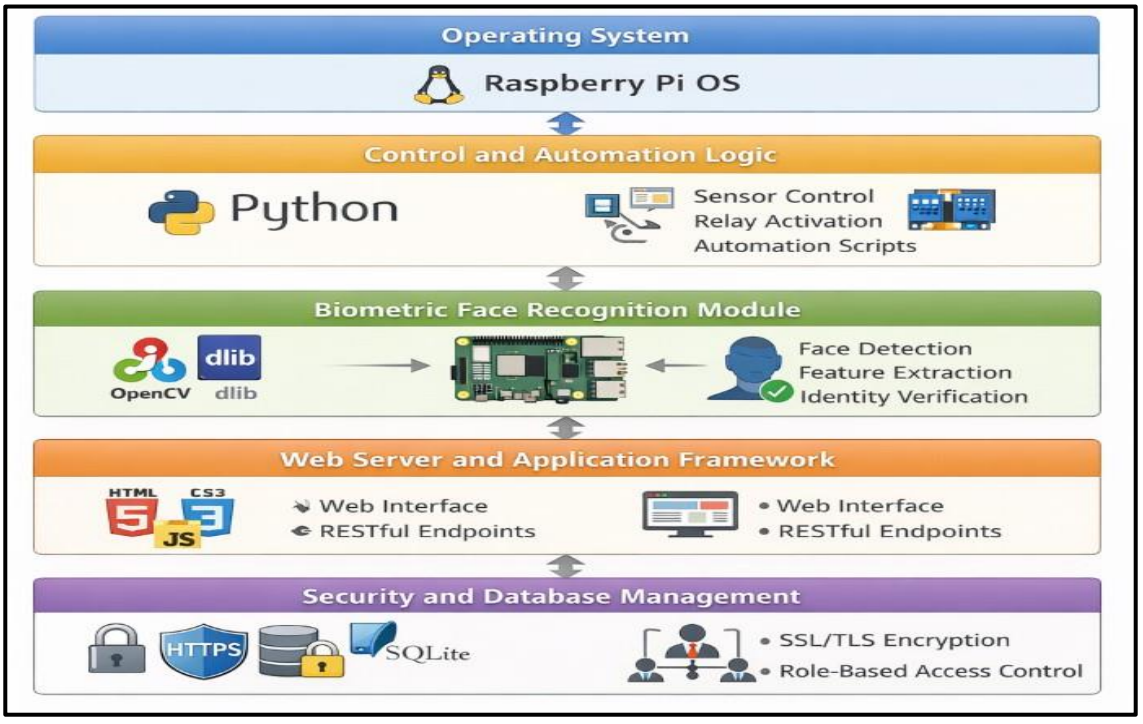


Figure 3. Software Implementation

• Biometric Face Recognition Software: The biometric recognition module is developed based on OpenCV and dlib. This is the module that realizes face detection, feature extraction, and identity verification. Facial features of authorized users are collected and stored privately in a local database during the enrollment phase. During the authentication, instant facial snapshots from the camera module are performed and compared with templates that were stored in advance. When a legitimate match is found, access is permitted by activating a corresponding control actuation. This software can run well on the embedded platform and performs the recognition at an acceptable level.

• Application Framework and Web Server: A slim web server is running on the Rasp- berry Pi itself to provide a web-based interface for controlling. The backend is exposed to the frontend application via RESTful endpoints and allows access to web containers of standard web technologies, HTML, CSS, and JavaScript. The server is responsible for accepting input requests, authenticating users, and passing control commands to the automation layer. This system allows homeowners to surveil and interact with appliances in their homes from an internet enabled media.

• Database and Data Management: Here, we hold local data in a small SQLite database. The database stores information about these: registered users; biometric data templates corresponding to the user's biometric attribute information, a device configuration, and system activity logs. This method provides a good balance between data access efficiency and resource

consumption such that it can be deployed in embedded systems. Sensitive information is secured using access controls, so any unauthorized release of information is avoided.

• Security, Access Control Software: Authentication and authorization mechanisms aim to implement security at the software level. Verifiable login steps are employed to restrict the system interface access only to authenticated users. Functionality limitation is enforced based on user privileges, administrator or regular user, using role-based access control (RBAC). Additionally, HTTPS can be used to securely communicate between the web interface and the Raspberry Pi using SSL/TLS for both data-integrity and confidentiality.

Each software component is combined to run as an entire system. User commands entered via the web interface, or requests for biometric authentication, are handled by the control logic, which receives them, approves them from the security module, and then executes them in the hardware control layer. Real-time system status updates and logs are produced and recorded in a database for monitoring and audit purposes. This unified approach facilitates the tight synchronization of software and hardware. A strong and secure base has been laid for the proposed automation system through the implementation of the software. With embedded control logic, biometric authentication, web-based interaction, and secure communications mechanisms mixed, a full software stack is developed to guarantee the efficient working of the system with scalable arguments and future improvements.

4.2 Biometric Face Recognition Module

In order to make the proposed IoT home automation system more secure, a biometric face recognition module is added for access control. This new module ensures secure user identification without physical keys or cards and provides a major enhancement to security and convenience. Figure 4 shows the workflow of the biometric face recognition module, illustrating image acquisition, face detection, feature extraction, and authentication decision for secure access control.

• Face Recognition Workflow: The biometric recognition in general works in a con- strained order of all image capturing, face detection, feature extraction, and identity verification. When a person requests access, the camera module automatically takes a real-time facial image of the user and sends it to the Raspberry Pi for processing. Authentication is executed locally to minimize latency and avoid reliance on the online cloud service.

• Face Detection: Face detection is realized with the OpenCV library, which detects face areas on captured image frames. A pre-trained detection model is adopted to detect faces juxtaposed by different illuminants and background situations. Detected face regions are normalized and made ready for feature extraction that remain same in successive authentications.

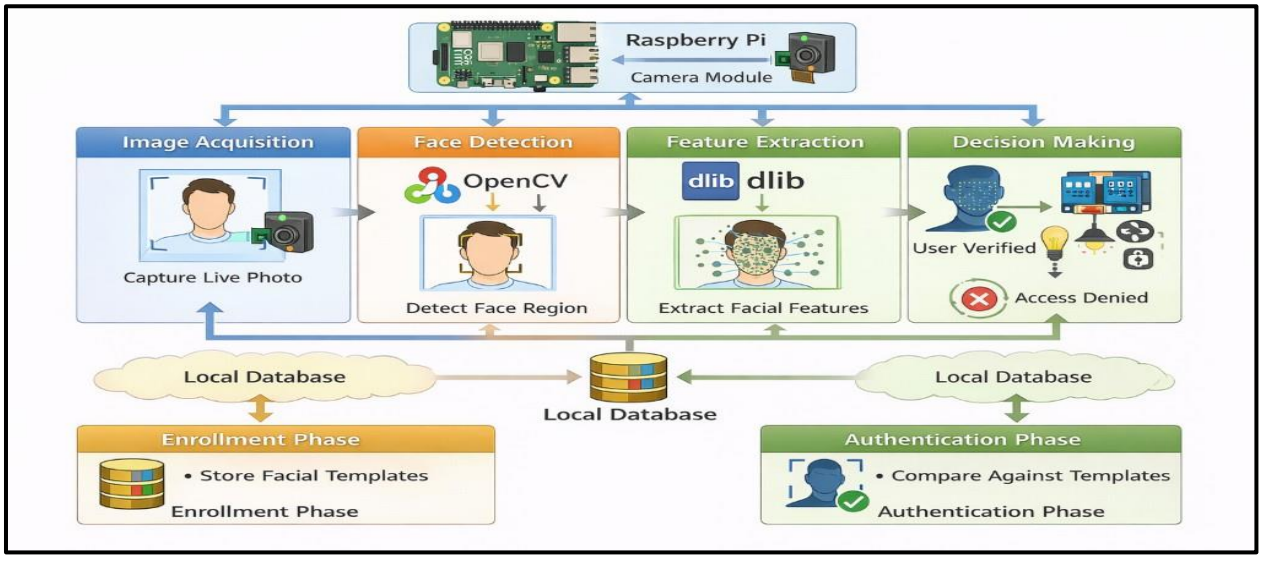


Figure 4. Biometric face recognition process used for system authentication

• Feature Extraction: When a face is detected, a unique set of noticeable facial features is found with the dlib library. Dlib produces an embedded facial representation through deep learning, which encodes a particular person's face that can be com- pared to another such encoding. The feature vectors are invariant under minor variations of pose and illumination, thus they are suitable for real-time embedded systems.

• Enrollment Phase: Authorized users are enrolled during the registration period by collecting their facial images in several photo shoots. Feature vectors are then computed and securely stored locally in a database. This phase constructs reference templates that act as ground truth for the following authentication trials.

• Authentication and Decision Making: During the phase of authentication, the feature vector is extracted from the live image, and it is matched against the templates using a similarity measure. The threshold is set at a similarity score; if the score of a frame exceeds this threshold, the user is authenticated successfully. If verification is successful, the system will activate the siren/buzzer light relay to allow granting or denying access through a doorway or a written turn-on warning of system relays. Unsuccessful login attempts are logged for monitoring and security review.

• Support for Home Automation Server. If home automation exists, then this smart plug can be connected to it and be controlled via home automation. One of the most attractive aspects is the system's embedded module of biometric face recognition, which coexists closely alongside reports and control layers. The results of an authentication directly affect the behavior of a system; therefore, only if the user is authenticated, the user may have control over appliances or access to restricted areas. It allows for biometric security to be perfectly coordinated with automation features that are IoT-purpose-based.

• Performance Considerations: The face recognition algorithm is fine-tuned to run on the Raspberry Pi. In this way, local processing reduces the latencies on the network, improving the responsiveness of a system. The modular architecture can also support future enhancements, such as integrating a more advanced deep learning model or multi-factor authentication, with minor changes in design.

The proposed IoT home automation system is easily capable of ensuring enhanced security through its noninvasive yet cost-effective protocol to validate the user's identity, which is based on a biometric face recognition technique. Thus, integrating real-time face detection, feature extraction, and secure decision making leads to reliable biometric access control that can be implemented in practical smart home applications.

4.3 Web-Based Control Interface

The web-based control interface is an important interaction medium between users and the envisaged IoT home automation system. It facilitates a centralized, user-friendly, and remote access platform for allowed users to check system status, control household appliances, set up scenes, and configure automation habits from the internet. Figure 5 shows the Web-based control interface of the proposed IoT home automation system, illustrating secure remote access, real-time device control, user management, and role- based access control.

• Interface Design and Structure: The user interface is implemented by using common web technologies like HTML, CSS, and JavaScript to achieve platform independence and easy usability. The interface is responsive in design and allows access from desktop, tablets, and Smart phone without the installation of additional software. The interface is structured in terms of functional modules - device control panels, system status indicators, and user management, enforcing clarity and convenience for navigation.

• Getting the Content from the Web Server and Integration with Backend: The web application is hosted on the Raspberry Pi as a server-side script with an upscaled web server. Request processing, user authentication, and communication with the automation logic layer are managed by backend services. When a user sends a control request from the interface, the request is checked and transferred to the Python- control module; this model runs an action on the hardware level. This server-side design enables command execution assurance with minimal round-trip time between users' commands and system responses.

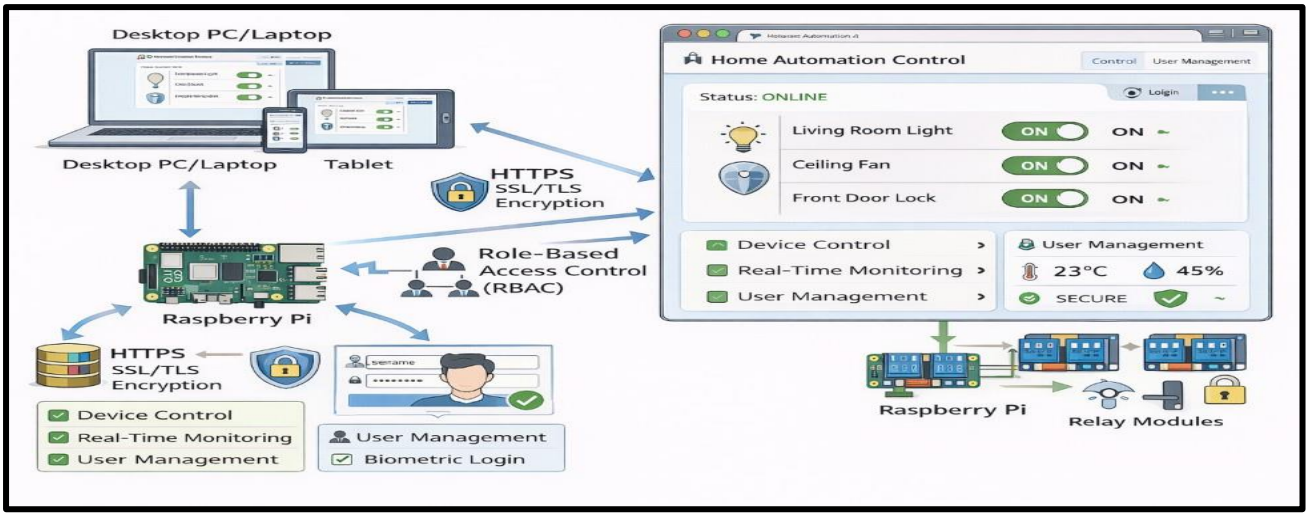


Figure 5. Web-based interface for remote monitoring and control of home appliances.

• Real-time control and monitoring of equipment: The web interface allows you to monitor and control your appliances in real-time. They can switch equipment ON or OFF, check the present system status, and get immediate feedback on the performed actions. Asynchronous communication methodology is used to dynamically update the status of the device and avoid the page from being reloaded, thereby improving responsiveness and user experience.

• User Authentication / Access Management: Not all users are able to access the web interface due to secure user authentication methods. The system requires authentication for any users wishing to access controls. Also, there is RBAC (Role-Based Access Control) implemented, where user privileges are defined, and administrative activities are only accessible to the authorized users. This method enhances the security of the system by deterring unauthorized people from performing control actions or changing setup information.

• Security and Communication Protection: All interactions with the web interface are secured via HTTPS using SSL/TLS, ensuring both data encryption and integrity possession. This will protect you from the most common eavesdropping and man- in-the-middle attacks. These vulnerable operations, such as login information and control commands, are transmitted securely for dependable operation of the system.

• Integration with Biometric Authentication: The internet of things controlling inter-face is linked with the biometric facial recognition module for security access. Biometric authentication outcomes have a direct impact on the scope of user privileges and guarantee that only authorized users can operate devices or access secured features. Such integration allows continuous control of a web-based system from biometric verification. The software program web-based control interface, a secure, user-friendly, and scalable interaction platform for the IoT ambient assisted living system, has been pro- posed. Through adopting responsive design, real-time control, secure communication, and access management based on biometric recognition, the interface largely improves usability and reliability of operation for the system.

4.4 Security and Communication Implementation

For IoT-based home automation systems, secure and dependable communication becomes a crucial necessity, especially for biometric data and remote access. The sys- tem provides a number of security designs to ensure the confidentiality of user data, to prevent unauthorized access, and for secure communications between components within the system. Figure 6 shows security and communication implementation of the proposed IoT home automation system, illustrating HTTPS-secured communi- cation, role-based access control, biometric authentication, secure device interaction, and system logging.

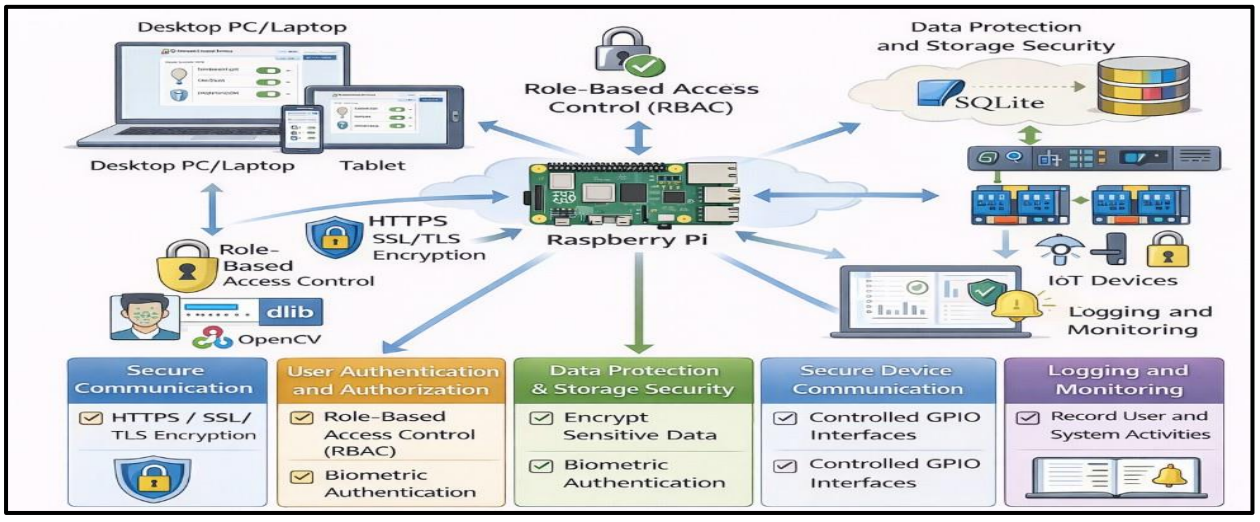


Figure 6. Security and communication framework of the proposed IoT home automation system

• Secure Communication Protocol: Every device-to-user communication with the Raspberry Pi is an HTTPS connection that has SSL/TLS encryption. This guarantees the confidentiality, the integrity, and authenticity of information that is transmitted, preventing eavesdroppers, replay attacks, and man-in-the-middle attacks. The encrypted communications channels are particularly useful for sending sensitive data, such as login credentials, biometric authentication results, and control messages.

• User Authentication and Authorization: The system is accessed using secure authentication processes. Users are required to log in prior to browsing the web application control interface. Besides traditional credential-based authentication, biometric face recognition is used as an extra protection measure for important access operations. It makes role-based access control (RBAC) for users, meaning administrators and regular user is implemented in a few seconds. Roles are given certain permissions such that users have access only to functions that belong to their privileges. This method reduces the potential of unauthorized manipulation of the system.

• Data Privacy and Storage Model: Critical system information, such as user pass- words, biometric templates, and audit logs, is stored on the RPi locally in a secure database. Access to stored data is limited through the use of size record attributes organized by size devices that can be used to specify who is denied access. The local data processing and storage function effectively mitigates the risk of external security threats, such as those presented through cloud services.

• Secure Device Communication: Tight control over GPIOs interfaces while send- ing commands to the IT devices provides bi-directional communication with the Raspberry Pi and connected IOT devices like contact sensors or relay modules. Com- mands are only processed if you've successfully authenticated /authorized yourself first, so device control actions are from a trusted source. This disables unwanted appliance triggering and improves overall system security.

• Logging and Monitoring: The software logs all users' activities, access attempts, and commands. These logs facilitate traceability and help in system watching, audit- ing, and troubleshooting. Authentication failures and unusual system behaviour are logged to aid the detection of possible security breaches.

With encrypted communication, secure authentication mechanisms, role-based access control, and data security handling, the proposed system demonstrates a prac- tical security mechanism for a smart home. Its security and communication protocols are built in so that the system remains resilient to all common cyber threats and yet is cost-effective for robust operation.

5. Experimental Results and Discussion

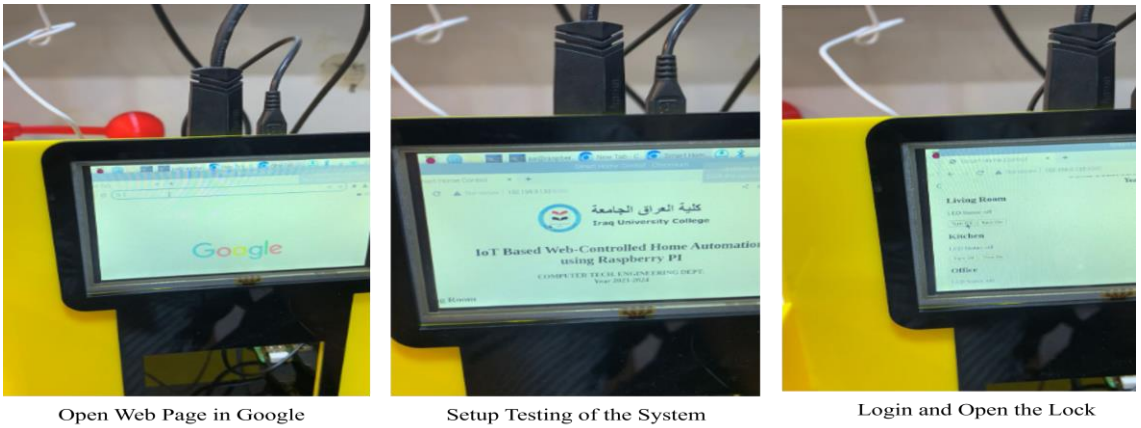
This section demonstrates the experimental validation of the introduced secure and scalable IoT home automation system in terms of performance, reliability, and security. The system was evaluated under realistic deployment conditions in order to confirm its malfunction and response capabilities.

5.1 Experimental Setup

The remote control was established by a Raspberry Pi 4, which was used to send wireless orders via the RSPi Camera module and the NRF24L01 detachable sensor. The service was linked to a local network, facilitating access via the web using different client devices such as PCs, tablets, and smartphones. The whole experimental setup is shown in Figure 7, whereas the software architecture is running on the Raspberry Pi.

• Biometric Authentication Performance: The biometric face recognition system was tested for authentication reliability and response pattern. During the experiments, users were registered to the system, and five trials for each user were conducted under normal indoor lighting conditions. The biometric processing chain, which consists of image acquisition, face detection, feature point extraction, and decision procedure. According to experimental results, the system was able to discriminate between authorized and forbidden users and initiate proper control actions accord- ingly. The authentication checks were performed on the Raspberry Pi to minimize latency and enhance system response time.

• Web Interface Responsiveness: Control response was analyzed by controlling com- mands sent from different client devices to the web-based control interface. We received immediate feedback for device status changes, verifying that the communi- cation between UI and control logic worked as designed. The choice of asynchronous handling for requests meant that device states could be updated in real-time without the need for page refresh, improving user experience immensely.



Open Web Page in Google | Setup Testing of the System | Login and Open the Lock

Figure 7. Result Project

• Security and Communication Evaluation: The security features built into the system were tested in production. All communication between users and the server was done over encrypted channels. HTTPS System functionalities were appropriately blocked based on user privileges, which were implemented by role-based access control to avoid unauthorized control commands. Also, authentication trials and control procedures were logged in system logs, which allowed traceability and support of monitoring and auditing features

6. Future Directions and Open Issues

It is evident that the IoT home automation agency's web-based and biometric control offers robust performance and enhanced system security; however, some open problems and future research areas should be addressed in order to further increase the reliability, scalability, and applicability of such a solution.

• Scalability and Multi-User Support: The above system is examined in a smart home test bed on reportage and actual application. Scalability in the form single deployment covering a larger deployment, with multiple rooms or buildings, or to distributed smart home nodes can be explored in future work. Simultaneous multi-user access of returned instantiations and high-rate control requests may need load-balancing approaches or distributed processing configurations.

• Advanced Biometric Robustness: Even though the biometric face recognition module is effective in normal indoor conditions, it may fail when unusual lighting conditions such as shadow or excessive light exist, an obstruction appears on the face, and a subject's appearance changes. Future work could also involve more sophisticated deep learning–based face recognition systems as well as multimodal biometric approaches (eg, face and voice fusion) in order to enhance robustness and authentication performance.

• Privacy and Data Protection preservation: Privacy is an issue in the biometric data processing. While behavioral biometric cues are processed locally, forthcoming systems may investigate privacy-enhancing mechanisms such as the use of template protection for biometrics, homomorphic encryption, and/or/and federated learning to lower the vulnerability of the sensitive data exposure zone. Furthermore, compliance with new data protection laws is still an issue.

• Edge–Cloud Integration: To achieve low latency and improve privacy, the proposed system follows a completely edge-based processing paradigm. Nonetheless, hybrid edge–cloud architectures could be applied in the future to facilitate data analytics, long-term adoption monitoring, and intelligent automation. The task offloading mechanisms among the edge devices and cloud servers are still open research problems.

• Intelligent Automation and Predictive Control Based on the above Reasoning, if we can monitor (with the help of intelligent sensors) and feed this information into an AI-based platform, such that a predictive analysis is conducted, enabling preemptive response and prevention of future failures before even actual occurrence.

• Cybersecurity and Attack Resilience: Despite applying encrypted communication and role-based access control, the security of IoT platforms cannot escape the tide of emerging cyber threats. In the future, intrusion detection systems, blockchain- based access control systems, or post-quantum crypto could be investigated to add layer of defense against sophisticated adversaries.

• Energy Efficiency and Resources Optimization: Constant work of cameras, sensors, and coprocessors could increase the amount of consumed energy. In the future, such energy-aware scheduling, adaptive sensing, and low-power hardware optimization need to be investigated further in order to sustain these systems for long times, especially on battery-based deployments.

• Interoperability and Standardization: It is still a challenge to interoperate with other third-party smart home platforms and heterogeneous IoT devices. There may be more advantages to be found for standardized communication protocols and middleware solutions so as to smoothly integrate different smart home settlements in the future.

7. Conclusion

This paper introduced a secure and scalable web-enabled IoT home automation architecture that incorporates web-based control and secured biometric face recognition to make the system more usable as well as secure. The system architecture followed the Raspberry Pi-based control unit, modeled and implemented according to a layered design that ensures continuous interoperability among hardware features, software services, and user interfaces. The experimental study showed that the system is working effectively in a real smart home. The HW-SW combination allowed responsive device control, with a web-based interface giving secure and live access. The valid user was recognized successfully by the

biometric face recognition module based on a predefined workflow including the image capture, detection of face area, extraction of characteristic data, and decision-making process without the normal key or password.

With HTTPS-enabled secure communication and role-based access control applied, the system was more effectively protected against unauthorized access. The outcomes show that the proposed system provides an affordable and realistic way for the implementation of smart home automation combined with improved security. In processing biometrics at the edge, it cuts back on latency and protects privacy. Furthermore, it is modular, and other devices, security layers, or smart automation capabilities can be added in the future. In conclusion, this work provides a proof of concept that IoT technologies, web GI, and biometrics can be effectively combined for the design of a secure, user-friendly smart home. This paper serves as a basis for future study and design for intelligent, scalable, privacy-aware home automation systems.

References

[1] Mishra, R., & Mishra, A. (2025). Current research on Internet of Things (IoT) security protocols: A survey. *Computers & Security, 151*, 104310.
[2] Schoder, D. (2025). Introduction to the Internet of Things. In *Internet of Things A to Z: Technologies and applications* (pp. 1–40).
[3] Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal, 6*(2), 2103–2115.
[4] Mohsin, A. S., Choudhury, S. H., & Muyeed, M. A. (2025). Automatic priority analysis of emergency response systems using Internet of Things (IoT) and machine learning (ML). *Transportation Engineering, 19*, 100304.
[5] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.
[6] Kokila, M., & Reddy, S. (2025). Authentication, access control and scalability models in Internet of Things security—A review. *Cyber Security and Applications, 3*, 100057.
[7] Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. *Smart Cities, 4*(3), 1196–1219.
[8] Bajaj, K., Sharma, B., Singh, R., Kumar, M., & Chowdhury, S. (2022). A comparative analysis of cloud based services platform. In *6th Smart Cities Symposium (SCS 2022)* (Vol. 2022, pp. 243–247). Institution of Engineering and Technology.
[9] Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of smart homes: Privacy and security. *Journal of Electrical and Computer Engineering, 2024*(1), 7716956.
[10] Yang, Q., & Wang, H. (2021). Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain. *IEEE Internet of Things Journal, 8*(14), 11463–11475.
[11] Hou, L., Zhao, S., Xiong, X., Zheng, K., Chatzimisios, P., Hossain, M. S., & Xiang, W. (2016). Internet of things cloud: Architecture and implementation. *IEEE Communications Magazine*, *54*(12), 32-39.
[12] Motta, L. L., Ferreira, L. C., Cabral, T. W., Lemes, D. A., Cardoso, G. D. S., Borchardt, A., Cardieri, P., Fraidenraich, G., De Lima, E. R., Neto, F. B., et al. (2023). General overview and proof of concept of a smart home energy management system architecture. *Electronics, 12*(21), 4453.
[13] Pahuja, S., & Goel, N. (2024). Multimodal biometric authentication: A review. *AI Communications*, *37*(4), 525–547.
[14] Hakim, I. M., Singgih, M. L., & Gunarta, I. K. (2023). Critical success factors for Internet of Things (IoT) implementation in automotive companies, Indonesia. *Sustainability*, *15*(4), 2909.
[15] Prakash, A. J., Patro, K. K., Hammad, M., Tadeusiewicz, R., & Pławiak, P. (2022). BAED: A secured biometric authentication system using ECG signal based on deep learning techniques. *Biocybernetics and Biomedical Engineering, 42*(4), 1081–1093.
[16] Gururaj, H., Soundarya, B., Priya, S., Shreyas, J., & Flammini, F. (2024). A comprehensive review of face recognition techniques, trends and challenges. *IEEE Access*.
[17] Boutros, F., Grebe, J. H., Kuijper, A., & Damer, N. (2023). IDiff-Face: Synthetic-based face recognition through fizzy identity-conditioned diffusion model. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (pp. 19650–19661).
[18] Zikria, Y. B., Ali, R., Afzal, M. K., & Kim, S. W. (2021). Next-generation internet of things (iot): Opportunities, challenges, and solutions. *Sensors*, *21*(4), 1174.
[19] Kaur, R., Vats, P., Mandot, M., Biswas, S. S., & Garg, R. (2021). Literature survey for IoT-based smart home automation: A comparative analysis. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1–6). IEEE.
[20] Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., Alkinani, M. H., Almazroey, A. A., & Gaber, T. (2024). FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. *Internet of Things, 25*, 101096.
[21] Rashdan, M., Almhaileej, H. Y. A., Almutairi, S. A., Ashkanani, F. K. E., Alhashimi, A. H., & Madoh, R. H. Y. (2025). IoT-based home automation system for smart living. In *2025 6th International Conference on Bio-engineering for Smart Technologies (BioSMART)* (pp. 1–4). IEEE.
[22] Al-Shareeda, M. A., Ghadban, A. A. H., Glass, A. A. H., Hadi, E. M. A., & Almaiah, M. A. (2025). Efficient implementation of post-quantum digital signatures on Raspberry Pi. *Discover Applied Sciences, 7*(6), 597.

[23] Salama, G. M., El-Gazar, S., Omar, B., & Hassan, A. (2024). Multimodal cancelable biometric authentication system based on EEG signal for IoT applications. *Journal of Optics, 53*(3), 1839–1853.
[24] Abd El-Rahiem, B., & Hammad, M. (2021). A multi-fusion IoT authentication system based on internal deep fusion of ECG signals. In *Security and privacy preserving for IoT and 5G networks: Techniques, challenges, and new directions* (pp. 53–79). Springer.
[25] Arpitha, T., Chouhan, D., & Shreyas, J. (2024). Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications. *Journal of Engineering and Applied Science, 71*(1), 8.
[26] Singh, V., & Kant, C. (2022). Biometric-based authentication in Internet of Things (IoT): A review. In *Advances in information communication technology and computing: Proceedings of AICTC 2021* (pp. 309–317). Springer.
[27] Ghadekar, P., Pradhan, M. R., Swain, D., & Acharya, B. (2024). EmoSecure: Enhancing smart home security with Fisherface emotion recognition and biometric access control. *IEEE Access, 12*, 93133–93144.
[28] Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications*, *82*, 103748.
[29] Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z. (2021). Towards smart home automation using IoT-enabled edge-computing paradigm. *Sensors*, *21*(14), 4932.
[30] Devanathan, B., Mathala, N. K., Suyampulingam, A., & Ilango, K. (2024). Secure and energy-efficient smart home automation: A user-based fingerprint security system. In *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)* (pp. 1–6). IEEE.
[31] Jagtap, S., Shirke, S., Shinde, R., Sonkusare, R., & Weakey, S. A. (2024). Scalable client-server home automation over wireless networks. In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)* (pp. 1–5). IEEE.