Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.13 No.1, 2024, pp.27-40

© Centre for Research and Innovation
www.crijournals.org
DOI: https://doi.org/10.70112/ajcst-2024.13.1.4260

Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices

Ashkan Yaldaie[1], Jari Porras[2] and Olaf Drögehorn[3]
[1&2]LUT University, Lappeenranta, Finland
[3]Harz University of Applied Sciences, Wernigerode, Germany
E-mail: ashkan.yaldaie@student.lut.fi

(Received 3 March 2024; Revised 23 March 2024; Accepted 13 April 2024; Available online 18 April 2024)

***Abstract* - As our homes become increasingly interconnected with smart devices, managing this technological complexity has never been more challenging. In response, this paper outlines an innovative approach to home automation using the versatile Raspberry Pi platform to address the unique needs of modern households. The research adopts a design science approach, starting with a thorough analysis of the challenges associated with the growing number of smart devices. The need to manage and control these devices drives the development of effective solutions. Various designs are considered, leading to the selection of the Raspberry Pi due to its flexibility and capability to integrate different smart devices into the automation process. To provide a comprehensive solution that simplifies device management and benefits users, the development process includes both hardware and software components. Additionally, a rigorous testing program is implemented to ensure that the system meets key requirements such as security, privacy, energy efficiency, and user-friendliness. The system's effectiveness is evaluated through real-world applications, which helps identify potential areas for improvement and iterative enhancement.**

***Keywords:* Smart Home, Home Automation, IoT, Remote Monitoring, Home Security, Energy Efficiency**

I. INTRODUCTION

The reliance of modern homes on smart gadgets is growing [1], presenting several issues, including the difficulty of controlling and monitoring these devices, concerns about security and privacy [2], [3], and the potential for inefficient energy use [4], [5]. This research offers a unique solution to these problems by using the Raspberry Pi to build a home automation system. Created by the Raspberry Pi Foundation, the Raspberry Pi is a small, credit card-sized computer designed to be an accessible and affordable platform for various DIY projects and educational purposes. Despite its small size and low cost, the Raspberry Pi offers remarkable computational capability, making it a great option for applications like home automation [6].

In this research, we investigate how a Raspberry Pi can be seamlessly integrated with a range of sensors to create a comprehensive system that enhances home automation. Our methodology incorporates considerations for security, privacy, energy efficiency, and user experience, demonstrating how this integration can result in a smarter and safer home for homeowners.

A. Problem Statement

The number of smart devices in homes is growing rapidly. In 2020, the global market for smart home devices was valued at USD 78.3 billion [7]. This value is expected to reach USD 135.3 billion by 2025. This growth is driven by several factors, including the increasing availability of affordable smart devices, the rising popularity of smart home platforms, and the growing demand for convenience and security [7]. While the use of smart devices offers numerous benefits, it also introduces some challenges. One of the most significant challenges in smart home systems is the complexity of managing and monitoring the diverse array of devices. With numerous devices in use, keeping track of their connections, activities, and security can be daunting. Typically, these systems rely on a central hub for device control and monitoring. However, they often exhibit certain limitations, including:

1. They can be expensive
2. They can be difficult to set up and use
3. Devices from different manufacturers may not always be compatible

Security and privacy are two significant concerns associated with the use of smart devices. These devices are typically connected to the internet, making them vulnerable to cyberattacks. Additionally, the data collected by smart devices can be exploited to track user behaviour and habits, raising valid privacy concerns. Finally, the use of smart devices can lead to energy waste. Many smart devices are designed to remain always on, even when not in use, resulting in unnecessary energy consumption that can negatively impact the environment [3].

B. Research Questions

The following research questions will be addressed in this study:

RQ1. How can a Raspberry Pi-based home automation system effectively prioritize security, privacy, and energy efficiency?

RQ2. What Metrics and Methods can be used to Assess the Effectiveness of this System in Improving User Experience and Reducing Energy Consumption?

The first research question (RQ1) addresses the key challenges of designing and developing a home automation system that ensures both the physical security of the house and the cybersecurity of the system itself, while also maintaining energy efficiency and user engagement. Security is a major concern for many people regarding home automation systems, as cybersecurity threats pose risks such as unauthorized access, data theft, or potential physical harm through device manipulation. Additionally, privacy concerns arise from the extensive data that home automation systems can collect on users' habits and activities [2], [8].

The second research question (RQ2) aims to measure the impact of a home automation system on users' lives. Such a system can enhance the overall user experience by simplifying device control and automating tasks. It can also reduce energy consumption by turning off lights and appliances when they are not in use, thereby saving money on energy bills and reducing the environmental impact of home energy use. By addressing these questions, this paper provides valuable insights into the design, development, and effectiveness of home automation systems. This information can be utilized to improve the security, privacy, energy efficiency, and user experience of these systems.

C. Methodology

The methodology employed in this study adheres to the principles of Design Science Research (DSR). DSR is a structured approach used to develop and evaluate innovative artifacts, such as systems or solutions, to address specific real-world problems. In this research, DSR provides the foundation for creating and assessing an integrated smart home security and resource management system.

The research process unfolds through a series of structured phases.

1. *Problem Identification:* The research begins with the identification of a pertinent real-world problem, which is the multifaceted need for contemporary homeowners to enhance home security, optimize resource consumption, and improve the overall user experience.
2. *Artifact Design and Development:* In response to the identified problem, an innovative artifact is designed and developed. This artifact constitutes the integrated smart home security and resource management system. The design process entails a comprehensive exploration of hardware and software components, with a focus on security, resource management, and user experience.
3. *Evaluation:* The system undergoes rigorous evaluation to assess its effectiveness in addressing the identified problem. Evaluation criteria encompass enhanced home security, resource management, and user experience.
4. *Reflection and Communication:* The research findings, including insights derived from the design, development, and evaluation of the system, are thoughtfully reflected upon. The outcomes and contributions are then effectively communicated through this research paper.

D. Research Contributions

It is imperative to note that the methodology employed in this study combines the systematic rigor of design science with a practical focus on addressing real-world challenges. By following this methodology, the research endeavors to create a valuable and innovative contribution to the fields of home automation, security, and resource management.

Design Science provides a robust framework for crafting a novel system that not only fulfills user requirements but also confronts prevailing challenges [9]. This paper serves as an indispensable guide for developers seeking to devise pragmatic solutions for end-users. In this context, our primary focus is not only on the development of a comprehensive home automation system but also on guiding others, ensuring that our goal extends beyond creating a system, but also serves as a valuable guide for those who wish to undertake similar endeavors.

II. RELATED WORK

In this section, the existing literature and research related to Raspberry Pi-based home automation systems, with a particular emphasis on security, privacy, and energy efficiency, are explored. The research discusses innovative systems and their contributions, vulnerabilities within the Raspbian operating system, as well as insights into user profiles, needs, and recommendations. This exploration provides essential groundwork for the Design Science Research approach, guiding the development of an enhanced product.

A. Raspberry Pi-Based Home Automation Systems

In recent years, there has been a significant surge in interest regarding the use of Raspberry Pi for creating home automation systems. The Raspberry Pi, an affordable single-board computer, is exceptionally well-suited for this purpose. Its user-friendly setup and extensive compatibility with a wide range of smart devices make it an attractive choice. One of the primary advantages of using this single-board computer in do-it-yourself (DIY) projects is its ability to enable the creation of highly personalized solutions tailored to individual requirements. This includes integrating cameras, various sensors, and GSM (mobile communications) devices into the Raspberry Pi, allowing it to handle a variety of tasks. Kumar *et al.,* present compelling evidence of how these sensors and devices, as shown in Fig. 2, can be leveraged to develop a home surveillance system [10].

Home automation systems place security and privacy at the forefront, as emphasized by a systematic literature review in the field [3]. This comprehensive analysis underscores users' deep concerns about protecting their private data, particularly given the inherent security vulnerabilities in smart home systems [2], [11], [12]. Additionally, the same body of research consistently highlights users' strong desire for efficient resource management, especially in the realm of electricity usage, as a potential way to reduce household expenses [4], [5]. Considering these concerns and needs, developers must prioritize allocating ample resources to strengthen the security features of home automation devices. Importantly, the enhancement of security should be a central consideration from the very beginning of the development process, starting with the planning and design phases. This proactive approach ensures that vulnerabilities are systematically identified and addressed, minimizing potential risks throughout the device's lifecycle [3].

B. Innovative Raspberry Pi-Based Systems

Shruti and Pallavi's home automation system represents an impressive fusion of smart surveillance and energy management, effectively addressing the twin concerns of security and resource optimization in contemporary households [13]. A standout feature of their system is the smart energy meter, which meticulously monitors and stores electricity consumption data. This empowers users with insights to make informed decisions, ultimately leading to reduced energy usage and lower household expenses. Additionally, their system offers remote accessibility, allowing users to conveniently control lighting, thereby enhancing both convenience and energy efficiency.

On the security front, their smart surveillance system records images when motion is detected. This dual-purpose feature acts as a deterrent to potential intruders and provides homeowners with a visual record of unusual activities. For real-time monitoring, users can access a live feed of their homes via the Pi Camera, a high-quality camera module designed for use with Raspberry Pi single-board computers. Despite their impressive prototype, Shruti and Pallavi recognize areas for future improvement, including refining the user interface, expanding remote control capabilities, and integrating advanced algorithms. Their work showcases the potential of seamlessly combining resource management and security in home automation [13].

In the realm of Raspberry Pi devices, Nadafa *et al.,* have pushed boundaries by introducing a security system with human detection capabilities, thereby reducing false security alerts triggered by motion detection [14]. Their innovative work extends to a smart mirror capable of delivering personalized messages to users, effectively enhancing both user experiences and home security measures. Nadafa and their team acknowledge the need for advanced programming expertise to optimize the system's performance and suggest that future iterations could address this limitation by implementing training mechanisms to distinguish legitimate users from potential intruders.

Teja *et al.,* focus their paper on safeguarding loved ones and valuables in household settings, recognizing the dynamic landscape of research and development in IoT applications for home security [15]. To address concerns about potential system compromise, they propose an innovative solution centred around the integration of four essential sensors: the Piezo sensor, IR sensor, PIR sensor, and Sound sensor. These sensors collectively enhance the system's ability to detect and respond to intrusions effectively.

At the core of Teja's system is the Raspberry Pi controller, which orchestrates the functions of these sensors with its 40 GPIO pins. This seamless integration allows for comprehensive threat detection, continuously monitoring the entire floor for any signs of movement. Once an intruder is detected, the sensors promptly capture images and videos, which are transmitted to the Raspberry Pi controller. This controller, with an Internet connection, relays this crucial information to the homeowner for remote assessment.

Furthermore, Teja *et al.,* emphasize the role of IoT technology in user interaction by integrating IoT Cloud for a graphical user interface (GUI) [15]. This GUI delivers real-time alerts and presents captured data, enhancing user-friendliness and accessibility. The paper also outlines potential enhancements, including delay alarms and advanced photo recognition technology, to reduce false alarms and increase system sensitivity for a more robust and reliable home security solution.

C. Operating System Security

In the paper authored by Le *et al.,* the researchers delve into the realm of operating system security, with a particular focus on Raspbian-OS for Raspberry Pi devices [16]. They underscore the significance of addressing vulnerabilities in Raspbian-OS, given the widespread use of Raspberry Pi across diverse applications. Identified vulnerabilities include default username and password combinations, software and hardware bugs, issues in various Raspbian-OS releases, and the susceptibility of secure shell (SSH) keys to attacks, all of which raise concerns about unauthorized access and potential data breaches.

To mitigate these vulnerabilities and enhance the security of Raspberry Pi-based systems, the authors propose several practical recommendations. They emphasize the immediate change of default credentials upon Raspbian-OS installation, replacing them with strong, unique username and password combinations. Regular software updates and patches are also suggested to rectify known bugs and security flaws. Additionally, the paper advocates for the implementation of strong authentication methods and the use of public key infrastructure (PKI) to enhance SSH key management. These proactive measures significantly reduce the likelihood of unauthorized access and safeguard sensitive data, fortifying Raspberry Pi-based devices in IoT environments [16].

In the paper authored by Sainz-Raso *et al.,* the researchers explore the security challenges associated with Raspberry Pi in the context of IoT [17]. They highlight that, despite its advantages, Raspberry Pi's reliance on operating systems exposes it to potential software vulnerabilities, and they discuss hardware limitations resulting from cost-cutting design choices during production. The paper meticulously analyzes various hardware and software vulnerabilities linked to different operating systems running on Raspberry Pi devices, emphasizing the importance of securing these systems in unprotected IoT environments.

To mitigate the identified vulnerabilities and enhance the security of Raspberry Pi-based systems, the authors propose a set of best practices. They recommend changing passwords immediately after installation and securing public services, especially when Raspberry Pi is exposed to the Internet. The analysis reveals that some default installations have unsecured services like FTP and HTTP, which can grant unauthorized access to attackers. The authors suggest removing unnecessary public services and advocate for secure configurations to minimize risks. In conclusion, the paper provides valuable insights into securing Raspberry Pi devices, benefiting engineers, developers, and designers working with this popular platform in various IoT applications [17].

D. User Profile and Adoption Concerns in Smart Home Technology

A recent survey-based study provides valuable insights into user profiles, adoption trends, and needs in the context of smart home technology [2]. The study reveals that the majority of participants are individuals in their 30s and 40s with university-level education, typically residing in rental accommodations. Although many respondents have heard of smart home technology, a significant number have not fully embraced it, indicating an opportunity for developers to explore the barriers to adoption. Future research is recommended to investigate the reasons behind this hesitation and to develop innovative strategies to address these concerns.

To promote adoption, developers are encouraged to invest in targeted marketing campaigns and educational initiatives that emphasize practical benefits such as increased security and convenience. The study also examines user needs and desired features in smart home systems. It notes that simple automation features, such as light control, are commonly used, while security features are highly desired. Participants expressed a desire for broader functionalities, including energy and water management, as well as task automation. This underscores the need for developers to prioritize and expand the range of features in their smart home products. Enhancing security aspects, integrating energy and water management functionalities, and enabling task automation can improve the overall user experience and appeal of smart home products [2].

Surveys [2], [18] identify participants' concerns related to reliability, high costs, privacy, and security issues associated with current smart home systems. This highlights the importance of developers prioritizing product reliability, addressing cost concerns, and enhancing privacy and security measures to build user confidence and encourage wider adoption. Furthermore, studies emphasize the significance of compatibility and integration of smart home systems with existing household products and appliances to reduce costs and enhance the user experience. Developers are urged to work towards interoperability and standardization in the smart home industry through collaborative efforts and partnerships among manufacturers.

In conclusion, studies provide a foundation for further research in the field of smart home development, addressing construct validity, internal validity, external validity, and reliability while acknowledging its limitations. They shed light on user preferences and potential areas for improvement in smart home technology, offering valuable guidance to developers in this evolving industry [2], [18].

E. Research Gaps

The extant body of literature offers valuable insights into various aspects of Raspberry Pi-based home automation systems. However, there is a significant research gap, as no comprehensive study currently addresses the interrelated domains of security, privacy, energy management, and user experience. The existing body of work predominantly focuses on discrete elements or specific facets of home automation, leaving a gap where a comprehensive investigation of these crucial dimensions is lacking.

It is uncommon to find research in the current literature that integrates the themes of security, privacy, energy efficiency, and user-friendliness in the context of Raspberry Pi home automation. While individual studies address specific topics such as user profiles [2], innovative systems [13], and operating system security [16], [17], the overall picture remains unclear. In summary, the existing research landscape does not provide the holistic investigation needed. The current study aims to bridge these dimensions, offering a richer understanding and contributing to the development of smarter, more efficient homes.

III. SYSTEM IMPLEMENTATION

The related work in the field of home automation systems has highlighted several key aspects. Researchers and developers have predominantly focused on two major areas: the development of new features and the enhancement of cybersecurity and data privacy. These two facets have been pivotal in shaping the evolution of home automation systems [3]. This paper aims to bridge the gap between these domains by creating a comprehensive system that integrates security features and data privacy measures while considering effective resource management. This approach recognizes the multifaceted needs of modern homeowners, who seek not only convenience but also assurance of a secure and efficient home environment.

The existing literature provides insights into the current landscape of home automation, showcasing innovative solutions that emphasize security and resource management. For example, Shruti and Pallavi's system [13], which integrates smart surveillance and energy metering, demonstrates the potential for seamlessly merging these aspects. Furthermore, the importance of addressing vulnerabilities in operating systems, as highlighted by Le *et al.,* and Sainz-Raso *et al.,* underscores the critical role of cybersecurity in the context of IoT devices like Raspberry Pi [16], [17].

This research aims to synthesize security, data privacy, and resource management, making a significant contribution to the field of home automation. By combining these elements, our work has the potential to create a more holistic and user-centric approach to smart homes, addressing the concerns and needs identified in the literature.

A. System Design

In this section, the system design phase of the research, guided by the principles of Design Science Research (DSR), is presented. The primary objective of this phase is to engineer a comprehensive home automation system that meets the overarching goals of this paper. In line with DSR principles, the aim is to create a novel system that not only addresses user requirements but also tackles existing challenges.

TABLE I OBJECTIVES

Integrating Privacy and Energy Monitoring	The first objective is to seamlessly integrate smart surveillance features with energy metering within the home automation system. This integration is crucial for addressing security and resource management in modern homes, providing users with the ability to monitor their homes through surveillance features while also efficiently managing their energy usage.
Fortifying Cybersecurity	The second objective is to fortify the security features of the home automation system. There is an acute awareness of the security vulnerabilities in smart home systems, and the aim is to proactively address these concerns. Security is a top priority [3], to ensure that vulnerabilities are identified and addressed systematically, minimizing potential risks throughout the device's lifecycle.
Enhancing Usability and Adoption	The third objective revolves around enhancing the user experience and addressing user concerns regarding smart home technology adoption. Recognizing the importance of user-centric design, the aim is to create a system that is not only secure and efficient but also user-friendly, encouraging wider adoption.

TABLE II PRINCIPLES

Modularity and Scalability	The design emphasizes modularity and scalability to allow for flexibility in expanding and customizing the system as per users' needs. The system's architecture is designed to accommodate additional components and functionalities.
User-Centric Design	User needs and preferences are prioritized, ensuring that the system is intuitive and easy to use. User-friendliness is a central focus throughout the design process.
Security by Design	Security is integrated into the system's design from the outset, following security best practices to minimize vulnerabilities and protect users' data and privacy.
Energy Efficiency	Incorporating energy-efficient components and features is a fundamental aspect of the design, aiming to help users optimize their energy consumption and reduce household expenses.

B. Hardware Setup

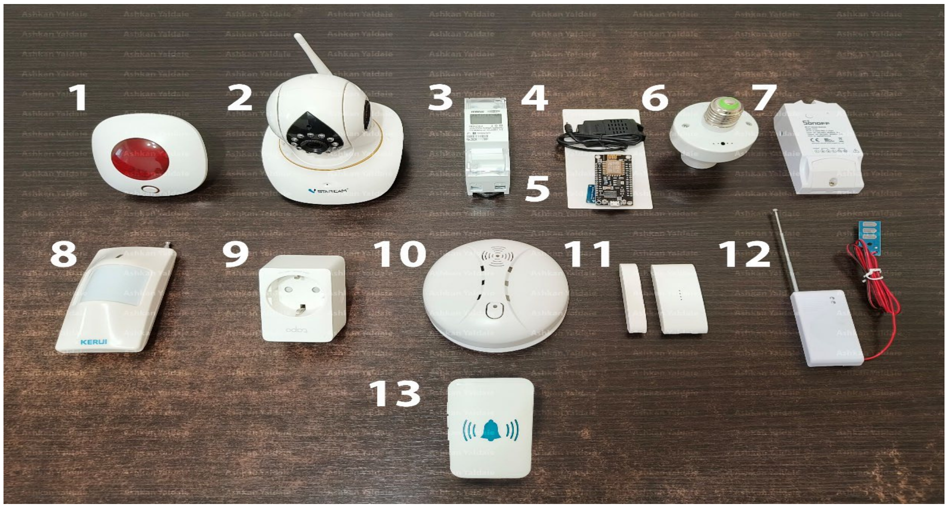


Fig.1 List of sensors and devices

1. Siren
2. IP Camera
3. Smart Electricity Counter
4. Temperature and Humidity Sensor
5. NodeMCU Board
6. Light bulb control device
7. Temperature and Humidity Sensor connector for transmitting the data
8. Motion Sensor
9. Remote Socket
10. Smoke Detector
11. Door Sensor
12. Water Leak Sensor
13. Doorbell Sensor

The hardware setup for this research project, as shown in Fig. 1, centers around the Raspberry Pi 3 Model B. This model was deliberately chosen due to its exceptional combination of processing power, memory, and versatile connectivity options. The selection of this model underscores our commitment to establishing a robust and efficient security system that seamlessly integrates user experience and resource management. This section provides a comprehensive exploration of the various hardware components meticulously integrated into our system, highlighting their crucial roles within the overarching framework.

1. *Motion Sensors:* Motion sensors are strategically placed throughout the premises to detect movements and trigger corresponding actions. Raspberry Pi 3 Model B interfaces with these sensors to receive real-time data.
2. *Remote Sockets:* Remote sockets, or smart plugs, enable remote control of electronic devices. They are integral to efficient resource management and can remotely activate lights and other home equipment.
3. *IP Cameras:* IP cameras serve dual roles, enhancing both home security and surveillance capabilities. Raspberry Pi connects to these cameras via the local network to capture and process video data.
4. *Smoke Detector:* A smoke detector is integrated into the system to enhance the smart home system. It promptly detects the presence of smoke, potentially signaling a fire hazard. Raspberry Pi is configured to receive and respond to signals from the smoke detector, triggering appropriate alerts and actions.
5. *Secure Housing for Raspberry Pi and Accessories:* To ensure the security and reliability of Raspberry Pi and its accompanying accessories, robust housing is utilized. This housing safeguards the components against physical harm and unauthorized access while maintaining a controlled environment for optimal performance.
6. *Incorporating GSM Modem for Security Alerts:* To ensure timely security alerts, a GSM modem is integrated into the system. This modem provides cellular connectivity, enabling the Raspberry Pi 3 Model B to send SMS notifications directly to the user in the event of a security intrusion, especially when Wi-Fi connectivity is unavailable. SMS is a text messaging service component of most mobile phones.
7. *NodeMCU Boards as Radio Frequency (RF) Signal Extenders:* To address limitations in RF signal coverage, strategically placed NodeMCU boards serve as signal extenders within the premises. These boards act as intermediaries, effectively expanding the RF communication range between the Raspberry Pi and other devices.
8. *Smart Electricity Counter for Resource Management:* Efficient resource management is facilitated through the integration of a smart electricity counter. This device tracks electricity consumption, providing valuable data for optimizing resource utilization.
9. *Temperature and Humidity Sensors:* These are integral components designed to monitor environmental conditions within the premises. These sensors provide real-time data on temperature and humidity levels, which are critical for user comfort. The system can adjust environmental settings, such as heating or cooling, based on this data, ensuring an optimal living environment and, in turn, enhancing user experience.
10. *Doorbell Sensor:* Further enhances home security and user convenience. This sensor is designed to detect and respond to doorbell rings. When triggered, it alerts the system, allowing for immediate user notification. This feature not only enhances security but also contributes to the overall user experience by providing a convenient way to monitor visitors and deliveries.
11. *Water Leak Sensors:* Water leak sensors are strategically placed to detect the presence of water in areas prone to leaks or flooding. These sensors promptly alert the system, helping to prevent water damage.
12. *Siren:* To provide an audible alert in case of security breaches or emergencies, a siren is integrated into the system. When triggered, the siren emits a loud alarm, alerting occupants and potentially deterring intruders. The siren adds a layer of security to the overall system.
13. *Door Sensors:* Door sensors are strategically placed at entry points throughout the premises. These sensors detect the opening of doors, providing crucial information about access points. Raspberry Pi interfaces with these sensors, promptly receiving status updates on door activities. The inclusion of door sensors enhances both security and user awareness, allowing the system to monitor and alert users to any unauthorized entry, thereby reinforcing the overall security posture.

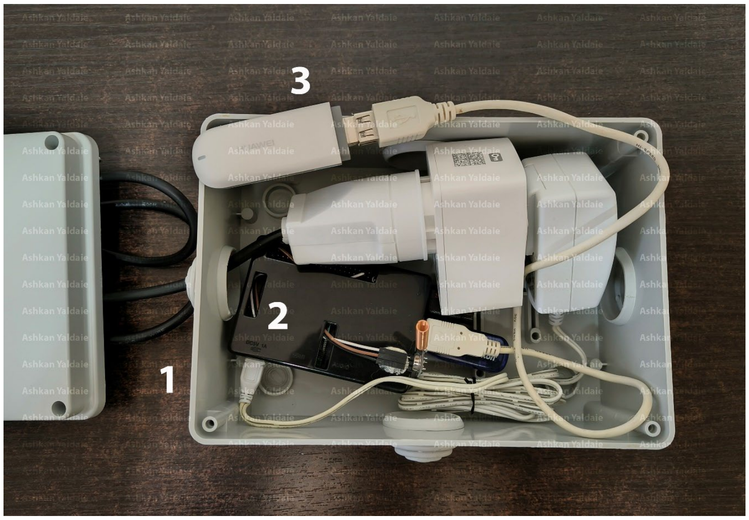


Fig. 2 Raspberry Pi and accessories

1. Secure Housing for Raspberry Pi and Accessories
2. The Raspberry Pi
3. Incorporating GSM Modem for Security Alerts

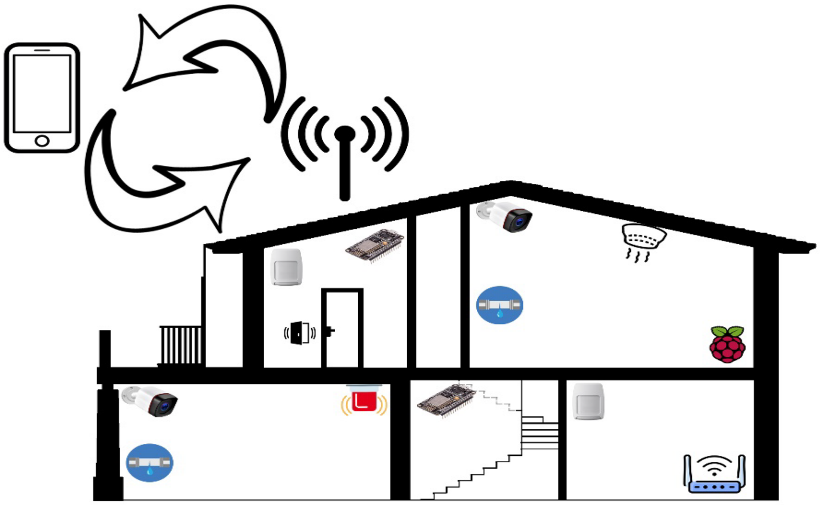


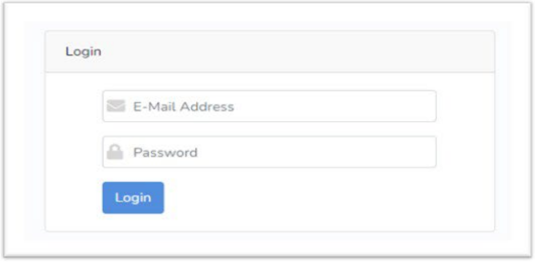
Fig. 3 Sensor placement in the house: a visual overview

In Fig. 3, a rough representation illustrates the placement of various house sensors, while Figs. 1 and 2 present lists of devices and accessories, accompanied by relevant illustrations. It is important to note that the communication infrastructure within the system plays a crucial role in ensuring seamless data transmission between the sensors and the central processing unit, the Raspberry Pi 3 Model B. In this context, radio frequency (RF) signals serve as the primary means of communication for most of the deployed sensors. To address the inherent limitations of RF signal range, NodeMCU boards have been strategically positioned within the premises. These NodeMCU boards function as signal extenders, effectively amplifying and expanding the RF communication range, thereby ensuring robust and uninterrupted data exchange between the sensors and the Raspberry Pi.

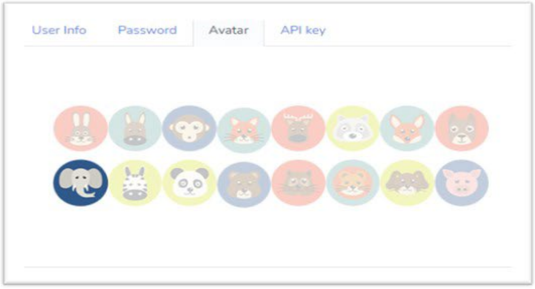
Additionally, it is essential to recognize that certain components within the system rely on Wi-Fi connectivity to communicate with the Raspberry Pi. Notably, IP cameras, the smart electricity counter, and temperature and humidity sensors utilize Wi-Fi technology for data transmission. This choice is driven by the specific requirements of these components, such as the need for higher bandwidth and the advantages of seamless integration into existing local area networks.

By harnessing Wi-Fi connectivity for these select devices, the system ensures efficient data conveyance to the central processing unit, contributing to the overall functionality and effectiveness of the integrated smart home security and resource management system.

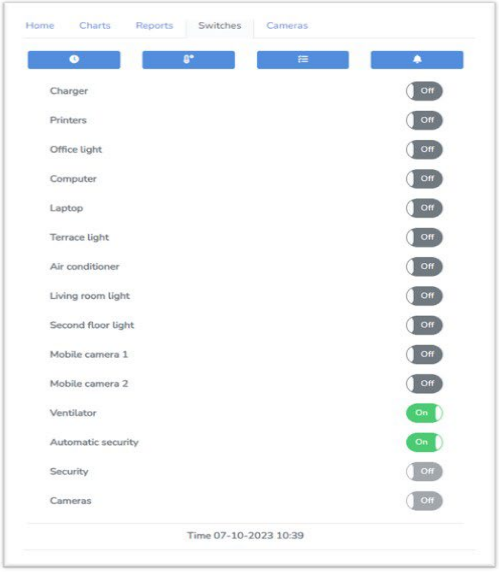
C. The Software



Login panel



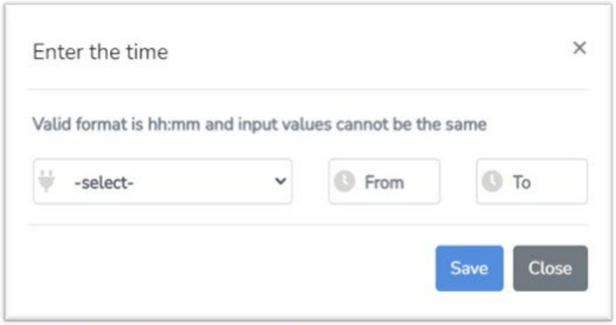
Profile view



Charger	Off
Printers	Off
Office light	Off
Computer	Off
Laptop	Off
Terrace light	Off
Air conditioner	Off
Living room light	Off
Second floor light	Off
Mobile camera 1	Off
Mobile camera 2	Off
Ventilator	On
Automatic security	On
Security	Off
Cameras	Off

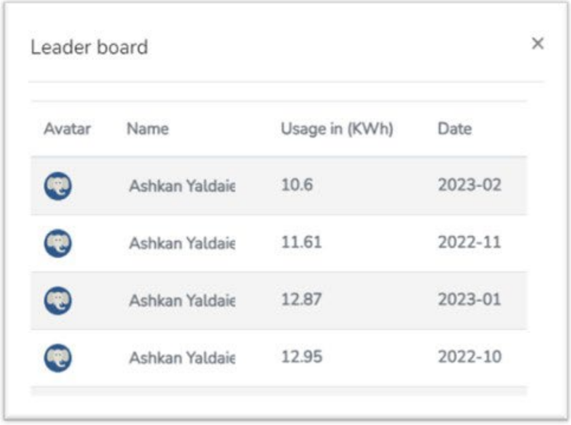
Time 07-10-2023 10:39

Control panel



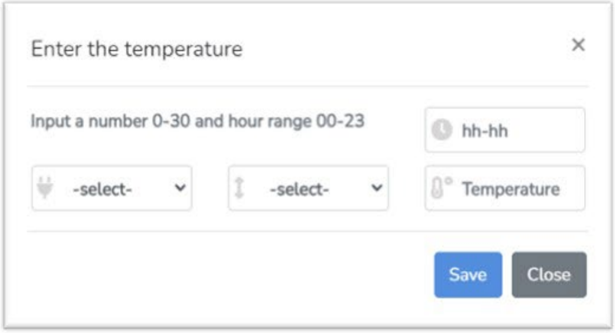
Valid format is hh:mm and input values cannot be the same

Control device power states using a time-based scheduling system



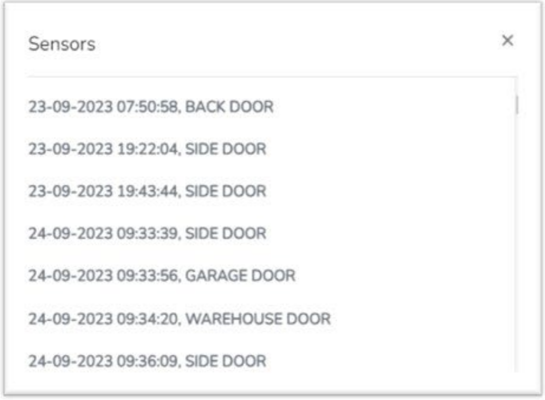
Avatar	Name	Usage in (KWh)	Date
	Ashkan Yaldaie	10.6	2023-02
	Ashkan Yaldaie	11.61	2022-11
	Ashkan Yaldaie	12.87	2023-01
	Ashkan Yaldaie	12.95	2022-10

Leaderboard for electricity usage



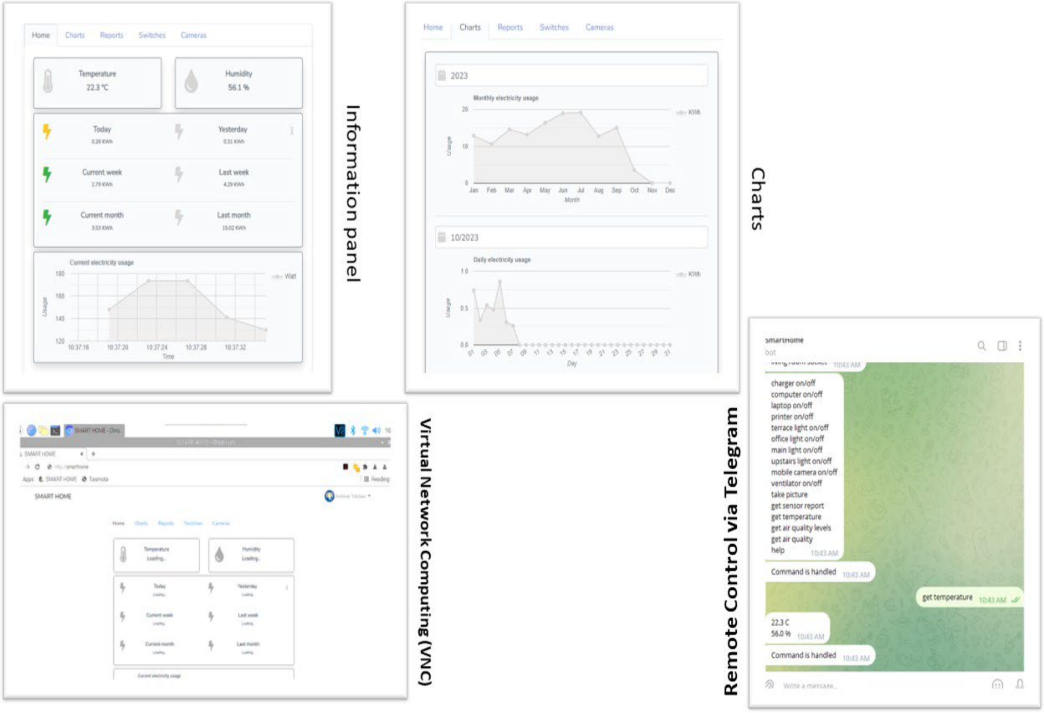
Input a number 0-30 and hour range 00-23

Regulate device operations according to temperature-based scheduling



23-09-2023 07:50:58, BACK DOOR
23-09-2023 19:22:04, SIDE DOOR
23-09-2023 19:43:44, SIDE DOOR
24-09-2023 09:33:39, SIDE DOOR
24-09-2023 09:33:56, GARAGE DOOR
24-09-2023 09:34:20, WAREHOUSE DOOR
24-09-2023 09:36:09, SIDE DOOR

History of triggered sensors



charger on/off
computer on/off
laptop on/off
printer on/off
terrace light on/off
office light on/off
main light on/off
upstairs light on/off
mobile camera on/off
ventilator on/off
take picture
get sensor report
get temperature
get air quality levels
get air quality
help 10:43 AM

Command is handled 10:43 AM

get temperature 10:43 AM

22.3 C
56.0 % 10:43 AM

Command is handled 10:43 AM

Fig. 4 Software in use

Fig. 4, titled "Software in Use," contains visual representations that showcase the practical application of the software within the system. As detailed in the preceding section, a diverse array of sensors and devices constitutes integral components within the system's architecture. This section shifts focus to the software development aspects that form the foundation for the effective integration and utilization of these sensors and devices. Specifically, it explores two key facets: system security and functionality. The first facet of this section is dedicated to system security. In an era where data breaches and cyber threats are persistent concerns, ensuring the utmost protection of user data and privacy is imperative. The intricacies of the cybersecurity measures implemented in the system - including encryption protocols, access controls, and intrusion detection mechanisms - will be thoroughly examined. The second goal of this section is to provide a comprehensive examination of the system's functionality.

This includes a detailed analysis of the operational aspects that facilitate the seamless integration and collaboration among the various sensors and devices. Additionally, it covers user interface and user experience considerations, highlighting how the system's design enhances user interaction and satisfaction. Furthermore, this section offers insights into the system's adaptability and scalability, elucidating how the architecture supports future expansions and modifications to maintain robustness and relevance in evolving technological landscapes. Finally, it addresses the system's performance metrics and optimization techniques, showcasing its commitment to achieving optimal resource utilization while maintaining high levels of efficiency and reliability.

1. System Security

Ensuring the cybersecurity of the Raspberry Pi-based security and automation system is of utmost importance for safeguarding both the device and the sensitive data it processes. In today's interconnected world, where cyber threats are pervasive, taking proactive measures to fortify the security of such systems is imperative. This section will delve into the comprehensive steps and best practices used to configure the Raspberry Pi with cybersecurity as a primary concern, providing a solid foundation for a resilient security infrastructure.

a. *Secure Operating System Installation:* The first critical step in securing your Raspberry Pi is the installation of a secure operating system. The authors have meticulously chosen Raspbian, the official Raspberry Pi OS, as the primary option. Selecting a minimal, hardened, and regularly updated distribution from official sources is essential. This approach minimizes the risk associated with compromised downloads and ensures the integrity of the system from the very outset.

b. *Modification of Default Credentials:* Following the installation phase, the authors have taken an additional step to fortify the system by modifying default credentials. Default usernames and passwords are known weak points in security. Robust and unique credentials have been adopted for accessing the Raspberry Pi, ensuring they are not easily guessable or common. This measure significantly raises the bar against potential unauthorized access attempts.

c. *Firewall Implementation:* The significance of implementing a firewall cannot be underestimated. In the ever-connected world of IoT devices, the Raspberry Pi requires a vigilant guardian in the form of a properly configured firewall. In this case, Uncomplicated Firewall (UFW) is the tool of choice. It is skillfully used to configure specific rules that restrict access exclusively to essential services, thereby minimizing exposure to potential threats.

d. *Regular Software Updates:* Security is a continuous journey, and regular software updates play a pivotal role in this ongoing process. The authors have made it a point to consistently apply security updates by keeping the operating system and software packages up to date. Automated update checks and installations have been configured to ensure timely patching and reduce vulnerabilities arising from outdated software.

e. *Enhancement of SSH Security:* SSH (Secure Shell) is employed for remote access, the default SSH port is modified to a non-standard value. Additionally, key-based authentication is configured in place of password-based authentication for heightened security.

f. *Intrusion Detection and Monitoring:* To truly fortify the security posture of the system, Intrusion Detection and Monitoring have been put into place. Robust intrusion detection systems (IDS) and monitoring tools continuously scrutinize system activity for signs of suspicion. Tools like Fail2ban automatically thwart repeated failed login attempts, further solidifying the system's resilience against potential threats.

By rigorously following these cybersecurity practices during the Raspberry Pi setup process, the system's security posture can be significantly strengthened. This enhancement serves as a robust defense against potential threats and vulnerabilities. It underscores the indispensable need for vigilant monitoring and continuous security updates in the ever-evolving landscape of cybersecurity, ensuring the safety of sensitive data and the integrity of the Raspberry Pi-based security system.

2. Remote Accessibility and Monitoring

The discussion in this section centers on the setup for controlling and monitoring the system. It explores the mechanisms employed to facilitate remote interaction with the home automation system, emphasizing the paramount importance of both security and usability. The implementation of various remote-control options, including Telegram integration, Virtual Network Computing (VNC), and a web-based user interface (UI), is meticulously examined.

These solutions are designed to provide users with seamless access to the system's functionalities while maintaining robust security measures. Additionally, the usability aspects of these choices are considered to ensure that user interactions with the system remain intuitive and efficient. By comprehensively addressing the setup for remote control and monitoring, this section underscores the commitment to delivering a holistic, user-centric, and secure home automation experience.

i. Remote Control via Telegram

Security Perspective	Usability Perspective
Remote control capabilities are an integral facet of our Raspberry Pi-based home automation system. To facilitate remote control while maintaining robust security, we have implemented Telegram integration. Telegram, a secure instant messaging platform, serves as the conduit for users to interact with the system from afar. Importantly, this choice aligns with our commitment to safeguarding the local network by avoiding the need to open any additional ports for external access. Telegram's inherent security features bolster the system's defense against unauthorized access. It employs end-to-end encryption for all communication, ensuring that messages exchanged between users and the system remain confidential.	Usability remains a pivotal concern in the design of our home automation system. Telegram's chat interface simplifies user interactions, reducing the learning curve for new users. Additionally, Telegram's cross-platform compatibility ensures that users can control the system from various devices, further enhancing usability. The system empowers users to monitor electricity usage, providing real-time insights into energy consumption. Users can seamlessly turn off devices remotely, promoting energy efficiency. Moreover, the system integrates temperature monitoring capabilities, allowing users to adjust heating or cooling systems based on real-time temperature data. This dual functionality not only enhances user convenience but also contributes to sustainable and energy-efficient living.

ii. Virtual Network Computing (VNC)

Security Perspective	Usability Perspective
Virtual Network Computing (VNC) serves as an additional component for remote system management. From a security standpoint, VNC incorporates password-based authentication to ensure that only authorized users can access the system remotely. Additionally, stringent access control measures are in place to limit the scope of remote interactions. Users must provide valid credentials to establish a VNC connection, further reinforcing security.	From a usability perspective, VNC offers a versatile solution for remote control. It enables users to access the system's graphical user interface (GUI) as if they were physically present, facilitating seamless interaction with the home automation system. This approach ensures a consistent and familiar user experience, which is especially valuable for tasks that require visual feedback or configuration adjustments.

iii. Web User Interface (UI)

Security Perspective	Usability Perspective
The web user interface (UI) is employed as an additional method for remote system management. From a security standpoint, it requires user credentials for access and operates within the local network without the need for port forwarding or exposure to external networks. This localized approach significantly reduces the system's attack surface, mitigating potential external threats.	The web UI provides a local control option for users within the network. It offers a simplified interface accessible through web browsers, allowing users to manage the system without needing VNC client software. This web-based approach enhances usability, particularly for users who prefer a browser-based interface.

3. Home Security Functionality

The home security functionality of the system comprises two key modes: Automatic Security and Continuous Security. When Automatic Security is activated, the system arms itself when the user(s) leave the house. This mode utilizes Bluetooth and Wi-Fi technology to monitor the physical presence of the user's phones, determining whether they are inside the house. By recognizing the absence of authorized devices, the system ensures that security measures are in place to safeguard the premises. In the interest of respecting user privacy, significant precautions have been taken regarding the security cameras.

When Automatic Security mode is active and the user(s) are at home, the security cameras are completely disconnected from the electrical supply. This deliberate action ensures that, during times when the system detects the presence of authorized users within the premises, the cameras are rendered inoperative. By cutting off their power, the system mitigates any potential privacy concerns that may arise from unintentional recording or monitoring while users are present.

This approach underscores the system's commitment to balancing security with the preservation of user privacy. Additionally, Continuous Security mode operates as an ongoing security measure, remaining armed until manually deactivated via the web interface. This persistent protection ensures that the property is consistently monitored, even when users are at home. To enhance security further, the system sends email notifications and SMS alerts to the user in the event of intrusion detection. These alerts provide timely awareness of potential security breaches. Alongside these notifications, a siren is activated to emit a Loud alarm, alerting occupants and potentially deterring intruders. The system also stores security camera clips of the intrusion, securely saving them in both local storage and Google Drive. This redundancy ensures that crucial evidence of security incidents is preserved and accessible, contributing to a comprehensive security posture.

4. Resource Management

The integrated smart home security and resource management system offers a range of functionalities designed to optimize resource consumption and enhance user awareness. These functionalities include dynamic control of devices based on temperature and specific timeframes, the generation of electricity usage reports, real-time monitoring of electricity consumption, and a traffic light system for comparative analysis.

A key feature of the resource management system is its ability to intelligently control devices based on temperature and specific timeframes. Users also have the flexibility to manually switch devices on or off using the provided on/off switches in the Web UI and through Telegram control. This dual functionality allows the system to automatically adjust devices for optimal energy use and user comfort while providing manual control for personalized adjustments. The system further supports detailed electricity usage reporting, offering users a comprehensive view of their consumption patterns. These reports include informative charts for selected timeframes, enabling users to gain insights into their energy utilization. Real-time monitoring is facilitated through a live chart, allowing users to track their electricity consumption as it occurs.

To enhance user awareness, the system features a traffic light system that compares current usage with historical data. This visual cue system uses colors that change from green to yellow and red based on usage compared to the previous day, week, and month. This intuitive feature helps users make informed decisions about their energy consumption and encourages energy-efficient practices. Additionally, the system includes a leaderboard that displays monthly electricity usage, fostering a sense of community and healthy competition. Users can choose avatars to represent themselves on the leaderboard, adding a personalized touch. This feature not only motivates users to conserve energy but also promotes data sharing and collaborative efforts toward sustainable living. The system leverages ThingSpeak, an open-source software for communication with internet-enabled devices. ThingSpeak is used to store and retrieve monthly usage data, providing a secure and accessible platform for sharing usage information.

IV. EVALUATION

The integrated smart home security and resource management system underwent rigorous evaluation to assess its performance, functionality, and usability in real-world scenarios. This evaluation process involved a series of tests conducted in a home environment, simulating various conditions to validate the system's effectiveness.

A. Security Evaluation

The Automatic Security mode, designed to activate when users leave their homes, underwent thorough testing. By leveraging Bluetooth signals from smartphones for user presence detection, the system consistently activated upon user departure, demonstrating robust detection capabilities. Notably, it exhibited a commendable ability to minimize false alarms when users were present, significantly enhancing the user experience.

Individual assessments of the intrusion detection mechanisms, including motion sensors and door sensors, were conducted to ensure prompt and accurate identification of unauthorized entry. The system reliably triggered alerts via email notifications and SMS messages, providing timely awareness of potential security breaches. Additionally, the integration of a siren in response to intrusions was validated, strengthening the overall security posture.

The innovative power management approach, which involves disconnecting security cameras from electricity when users are at home, was rigorously evaluated, particularly regarding its impact on user privacy. The deliberate disconnection during the Automatic Security mode ensured that security cameras remained inactive in the presence of users, effectively addressing potential privacy concerns.

B. Resource Management Evaluation

The resource management aspects of the integrated smart home security system underwent comprehensive testing to evaluate their effectiveness, usability, and impact on user experience. Real-time monitoring of electricity consumption proved effective, providing users with live data during periods of high electricity prices. This capability empowered users to make informed decisions about device usage, contributing to energy efficiency. The traffic light system, which indicates usage compared to historical data, offered an intuitive visual cue for regulating energy consumption.

The intelligent device control, based on temperature and predefined timeframes, demonstrated efficacy in optimizing resource utilization. Users could remotely turn off devices, even when away from home, contributing to energy efficiency during peak pricing periods.

The remote-control capabilities via Telegram, VNC, and the web-based UI were evaluated for usability and responsiveness, providing users with flexible and secure options for managing their smart home environment. Additionally, the leaderboard feature, which promotes a sense of achievement by comparing electricity usage to previous months, successfully added a gamified element through customizable avatars and monthly rankings.

C. Additional Tests

The range of radio frequency (RF) signals to reach the Raspberry Pi was tested in various locations within the home. This ensured that all sensors utilizing RF communication, including NodeMCU boards, operated within the required range, maintaining robust and uninterrupted data exchange. Each sensor - such as motion sensors, temperature and humidity sensors, door sensors, and water leak sensors - underwent individual testing. This approach ensured the reliability and accuracy of each sensor in detecting specific environmental conditions or events.

V. CRITICAL DISCUSSION

In this section, we conduct a critical examination of our integrated smart home security and resource management system, guided by the principles of Design Science Research (DSR). Our research aims to address the multifaceted needs of modern homeowners, prioritizing security, resource management, and user experience. We scrutinize the system's design, functionality, and contributions to the broader field of home automation, all while addressing the two core research questions posed in this study.

A. Research Question 1: How can a Raspberry Pi-Based Home Automation System Effectively Prioritize Security, Privacy, and Energy Efficiency?

Our integrated system significantly enhances home security through a combination of automatic and continuous security functions. The Automatic Security mode ensures that the system is armed when users leave their homes. This mode uses Bluetooth and Wi-Fi signals from user smartphones to determine their presence within the house. If users are not detected, the system activates, thereby fortifying the home's security. Notably, this approach reduces the likelihood of false alarms when users are present, improving the overall user experience.

Regarding security, the system employs intrusion detection mechanisms, email notifications, SMS alerts, and stores security camera clips both locally and on Google Drive. These robust security measures act as formidable deterrents to potential intruders and provide homeowners with timely awareness of security breaches. Additionally, the inclusion of a siren adds an audible layer of protection, boosting user confidence in the system's ability to secure their homes. The system's comprehensive approach to security also includes advanced cybersecurity features, as detailed earlier. By adhering to best practices-such as secure operating system installation, modification of default credentials, firewall implementation, regular software updates, SSH security enhancements, and intrusion detection and monitoring - the system ensures the utmost protection of user data and privacy. These cybersecurity measures form a solid foundation for a resilient security infrastructure, reinforcing the overall security posture of the integrated smart home security and resource management system.

An innovative aspect of the system's design is its power management approach, which prioritizes user privacy. When Automatic Security mode is active and users are at home, the security cameras are completely disconnected from the electricity. This feature addresses privacy concerns while maintaining vigilant security when users are away.

B. Research Question 2: What Metrics and Methods can be used to Assess the Effectiveness of this System in Improving User Experience and Reducing Energy Consumption?

Resource management is a critical aspect of our integrated system, providing a range of functionalities that empower users to optimize resource consumption. Users can intelligently control devices based on temperature and predefined timeframes, enhancing energy efficiency and contributing to cost savings. The system offers real-time monitoring of electricity consumption, complemented by a traffic light system that provides a comparative analysis of usage trends. This visual representation simplifies user awareness and decision-making, aligning with the principles of Design Science by offering intuitive feedback.

Additionally, the leaderboard feature fosters healthy competition among users to reduce electricity usage. This gamification element, which includes customizable avatars and user rankings, encourages active participation in resource management efforts. We have utilized ThingSpeak to store and retrieve monthly usage data, promoting user engagement and community sharing of usage information.

VI. CONCLUSION

In this study, we introduced an integrated smart home security and resource management system designed to meet the diverse needs of contemporary homeowners. Our exploration of the system's hardware and software components has provided insights into its architecture, demonstrating its potential to enhance home security and optimize resource utilization. It is noteworthy that our system is meticulously designed with an awareness of the constraints outlined in the related work section. The system's core strength lies in its ability to enhance home security through a combination of automatic and continuous functions. The Automatic Security mode uses Bluetooth signals to detect user presence, fortifying the home's security posture when users are away. This approach minimizes false alarms when residents are at home, contributing to an improved user experience. Additionally, intrusion detection mechanisms, email notifications, SMS alerts, and secure storage of security camera clips-both locally and in Google Drive-form a robust security ecosystem. The inclusion of a siren further augments security measures, instilling confidence in the system's ability to protect homes. Notably, the system also addresses user privacy by disconnecting security cameras from electricity when Automatic Security mode is active, and users are present at home. Cybersecurity remains a paramount consideration in the system's design, with stringent measures implemented to safeguard user data and privacy. The system adopts secure operating system installation, credential modification, firewall implementation, regular software updates, SSH security enhancement, and intrusion detection mechanisms to establish a resilient security infrastructure. In terms of resource management, the system offers dynamic device control based on temperature and specific timeframes, generates electricity usage reports, provides real-time monitoring, and employs a traffic light system for comparative analysis. These functionalities empower users to make informed decisions about resource consumption, potentially leading to cost savings and increased efficiency. To validate the practicality and effectiveness of our system, we deployed it in a real-world test environment. This validation phase allowed us to observe the system's performance in diverse scenarios, ensuring its effectiveness in the complexities of an actual home environment. However, we acknowledge certain limitations. Future iterations should consider that comprehensive home security ideally begins during the construction phase. Vulnerabilities, such as exposed electricity boxes that intruders can exploit to disable security systems, must be addressed. Innovative solutions, such as connecting critical components to power banks, may be necessary despite potential higher costs. A more holistic approach to securing vital infrastructure around electricity boxes is imperative for robust home security. In conclusion, our integrated smart home security and resource management system represents a significant advancement in meeting the evolving needs of homeowners. By combining advanced security measures with resource management capabilities, the system offers enhanced convenience, efficiency, and peace of mind for users. As technology continues to evolve, both homeowners and developers must prioritize security and resource management to create safer, more sustainable living environments.

REFERENCES

[1] R. El-Azab, "Smart homes: potentials and challenges," *Clean Energy*, vol. 5, no. 2, pp. 302–315, Jun. 2021, doi: 10.1093/ce/zkab010.

[2] A. Yaldaie, J. Porras, and O. Drögehorn, "Who are Smart Home Users and What do they Want? – Insights from an International Survey," *Appl. Comput. Syst.*, vol. 28, no. 1, pp. 114-124, Jun. 2023, doi: 10.2478/acss-2023-0011.

[3] A. Yaldaie, J. Porras, and O. Drögehorn, "The Present State of Home Automation: A Systematic Literature Review," *Int. J. Hybrid Innov. Technol.*, vol. 2, no. 1, pp. 23-46, Oct. 2022, doi: 10.21742/ijhit.2653-309X.2022.2.1.03.

[4] R. Rasheed, A. Ahmed, and F. Bukhari, "A survey base study about the effectiveness of smart home applications in Pakistan," in *2018 International Conference on Engineering and Emerging Technologies (ICEET)*, Feb. 2018, pp. 1-5, doi: 10.1109/ICEET1.2018.8338640.

[5] M. Z. Fakhar, E. Yalcin, and A. Bilge, "A survey of smart home energy conservation techniques," *Expert Syst. Appl.*, vol. 213, p. 118974, Mar. 2023, doi: 10.1016/j.eswa.2022.118974.

[6] X. Wen and Y. Wang, "Design of smart home environment monitoring system based on raspberry Pi," in *2018 Chinese Control*

And Decision Conference (CCDC), Jun. 2018, pp. 4259-4263, doi: 10.1109/CCDC.2018.8407864.

[7] R. and Markets, "Global Smart Home Healthcare Market (2020 to 2025) - Growth, Trends and Forecasts," 2021. [Online]. Available: https://www.globenewswire.com/en/news-release/2021/01/06/2154442/28124/en/Global-Smart-Home-Healthcare-Market-2020-to-2025-Growth-Trends-and-Forecasts.html

[8] J. I. I. Araya and H. Rifà-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," *Internet of Things*, vol. 22, p. 100792, Jul. 2023, doi: 10.1016/j.iot.2023.100792.

[9] A.-K. Carstensen and J. Bernhard, "Design science research – a powerful tool for improving methods in engineering education research," *Eur. J. Eng. Educ.*, vol. 44, no. 1-2, pp. 85-102, Mar. 2019, doi: 10.1080/03043797.2018.1498459.

[10] V. A. Kumar, V. Nandalal, M. Kousalya, P. Madhumitha, R. Kamaleshwari, and N. K. Selvi, "Implementation of Smart Home Assistance and Surveillance," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Mar. 2021, pp. 1117–1121, doi: 10.1109/ICACCS51430.2021.9442055.

[11] N. Pattnaik, S. Li, and J. R. C. Nurse, "A Survey of User Perspectives on Security and Privacy in a Home Networking Environment," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1-38, Sep. 2023, doi: 10.1145/3558095.

[12] D. Brand, F. D. DiGennaro Reed, M. D. Morley, T. G. Erath, and M. D. Novak, "A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities," *Behav. Anal. Pract.*, vol. 13, no. 1, pp. 11-21, Mar. 2020, doi: 10.1007/s40617-018-00329-y.

[13] S. Dash and P. Choudekar, "Home Automation using Smart Devices and IoT," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Sep. 2021, pp. 1-5, doi: 10.1109/ICRITO51393.2021.9596533.

[14] R. A. Nadafa, S. M. Hatturea, V. M. Bonala, and S. P. Naikb, "Home Security against Human Intrusion using Raspberry Pi," *Procedia Comput. Sci.*, vol. 167, pp. 1811-1820, 2020, doi: 10.1016/j.procs.2020.03.200.

[15] P. A. Teja, A. A. F. Joe, and V. Kalist, "Home Security System using Raspberry PI with IOT," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Mar. 2021, pp. 450-453, doi: 10.1109/ICACITE51222.2021.9404551.

[16] C. Le, A. M. Grande, A. Carmine, J. Thompson, and T. Khan Mohd, "Analysis of Various Vulnerabilities in the Raspbian Operating System and Solutions," in *2022 IEEE World AI IoT Congress (AIIoT)*, Jun. 2022, pp. 01-06, doi: 10.1109/AIIoT54504.2022.9817202.

[17] J. Sainz-Raso, S. Martin, G. Diaz, and M. Castro, "Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 47-52, Nov. 2019, doi: 10.1109/MCE.2019.2941347.

[18] M. Ghafurian, C. Ellard, and K. Dautenhahn, "An investigation into the use of smart home devices, user preferences, and impact during COVID-19," *Comput. Hum. Behav. Reports*, vol. 11, p. 100300, Aug. 2023, doi: 10.1016/j.chbr.2023.100300.