IoT

MDPI

Article

Development and Assessment of Internet of Things-Driven Smart Home Security and Automation with Voice Commands

Paniti Netinant [1], Thitipong Utsanok [1], Meennapa Rukhiran [2,*] and Suttipong Klongdee [2,*]

[1] College of Digital Innovation Technology, Rangsit University, Pathum Thani 12000, Thailand; paniti.n@rsu.ac.th (P.N.); thitipong.u65@rsu.ac.th (T.U.)
[2] Faculty of Social Technology, Rajamangala University of Technology Tawan-ok, Chanthaburi 22210, Thailand
* Correspondence: meennapa_ru@rmutto.ac.th (M.R.); suttipong_kl@rmutto.ac.th (S.K.); Tel.: +66-80-954-2898 (M.R.)

Abstract: With the rapid rise of digitalization in the global economy, home security systems have become increasingly important for personal comfort and property protection. The collaboration between humans, the Internet of Things (IoT), and smart homes can be highly efficient. Interaction considers convenience, efficiency, security, responsiveness, and automation. This study aims to develop and assess IoT-based home security systems utilizing passive infrared (PIR) sensors to improve user interface, security, and automation controls using voice commands and buttons across different communication protocols. The proposed system incorporates controls for lighting and intrusion monitoring, as well as assessing both the functionality of voice commands and the precision of intruder detection via the PIR sensors. Intelligent light control and PIR intruder detection with a variable delay time for response detection are unified into the research methodology. The test outcomes examine the average effective response time in-depth, revealing performance distinctions among wireless fidelity (Wi-Fi) and fourth- and fifth-generation mobile connections. The outcomes illustrate the reliability of voice-activated light control via Google Assistant, with response accuracy rates of 83 percent for Thai voice commands and 91.50 percent for English voice commands. Moreover, the Blynk mobile application provided exceptional precision regarding operating light-button commands. The PIR motion detectors have a one hundred percent detection accuracy, and a 2.5 s delay is advised for PIR detection. Extended PIR detection delays result in prolonged system response times. This study examines the intricacies of response times across various environmental conditions, considering different degrees of mobile communication quality. This study ultimately advances the field by developing an IoT system prepared for efficient integration into everyday life, holding the potential to provide improved convenience, time-saving effectiveness, cost-efficiency, and enhanced home security protocols.

Keywords: home automation; home security system; Internet of Things; intruder detection; PIR sensor; smart home; voice commands

Citation: Netinant, P.; Utsanok, T.; Rukhiran, M.; Klongdee, S. Development and Assessment of Internet of Things-Driven Smart Home Security and Automation with Voice Commands. *IoT* **2024**, *5*, 79–99. https://doi.org/10.3390/iot5010005

Academic Editor: Amiya Nayak

Received: 31 December 2023
Revised: 25 January 2024
Accepted: 29 January 2024
Published: 1 February 2024

1. Introduction

Crime continues to be a prevalent issue with significant economic, social, and political consequences in countries across the globe [1]. Approximately 83% of the world's population resides in areas characterized by elevated levels of criminal activity [2]. Contemporary home security systems have undergone significant advancements, expanding the system's reach beyond mere residential protection by integrating home automation capabilities. Incorporating these modern features helps improve security measures, provides convenience to consumers in their daily lives, and contributes to endeavors aimed at convenience and energy conservation.

In our rapidly evolving digital age, the Internet of Things (IoT) has emerged as a critical smart application for modern security living [3–9]. Integrating IoT devices, automation

detection, and notification systems with smart home technology offers a comprehensive security solution for everyday activities [8,10,11]. Cost optimization and facilitation are significant benefits provided by IoT-driven transformations for real-time remote-access systems [12] through cellular and Wi-Fi networks [4,6,13]. Integrating mobile access points within an IoT-driven home security system can significantly enhance the system's ability to manage energy resources and maintain robust communication with various sensors and devices. By dynamically adjusting to the optimal positions within a home, these mobile access points ensure that the system's throughput is maximized, resulting in a more responsive and energy-efficient security network [14,15]. The integration of IoT technology and internet connectivity enables users to remotely manage and react to smart home security system functions, including appliance control, security monitoring, intrusion alert, and automation lighting control [4,6,12,16].

Furthermore, incorporating energy monitoring and control is essential in designing and developing smart home security [17–19]. Smart home security systems are implemented using a single-board computer (SBC) to reduce energy consumption effectively. Famous microcontrollers, including but not limited to Raspberry Pi, Arduino, and ModeMCU, propel progress in the IoT domains of smart homes and security [7,20–24]. The compatibility of lighting management and intrusion detection exemplifies the revolutionary capacity of IoT technologies. Alarms throughout the property may be automatically illuminated or sounded upon the detection of an intruder by a hub. This interconnectivity improves security, so the responsiveness of IoT systems and user alerts demonstrate how the requirements for home safety are strengthened. Existing studies [25–28] have established that integrating IoT-enabled PIR (passive infrared sensor) intrusion detection into home automation systems positively influences security by providing comfort, energy, responsiveness, cost savings, remote control, and convenience.

Similarly, customizing smart home security systems to cater to the most stringent user demands poses unique obstacles, particularly concerning hands-free dictation. The use of voice-activated commands has transformed both automation and human-liberated control. Voice recognition technology has surfaced as a potentially effective intelligent security application for enhancing user convenience and natural command methods. Based on our previous research [29], an earlier study proposed IoT-enabled intruder detection via voice and motion to support a smart light. When an intruder was spotted via a PIR sensor, the system could activate the relay to switch the lights on or off. The research results were observed and summarized on user commands via the Blynk button and Google voice assistance in Thai and English during varying delay times of PIR sensors. However, the prior research gap of voice-activated commands in different wireless network communications, accuracy, responsiveness, detection angles, and multilanguage supports through the smart home security and automation system can continuously be explored for further motivation.

Therefore, this study aims to design an IoT-based home security framework, develop system operations, and investigate accuracy, responsiveness, and outcome sensor delays using PIR sensors to support hardware, processes, and systems for enhanced user interaction and system control through voice and button commands in various communication technologies. The IoT-based proposed framework can improve and optimize lighting and security management by utilizing voice and buttons developed on Raspberry Pi to detect intruder motions. The research methodology includes hands-on experiments to evaluate the precision and responsiveness of the system under typical user-controlled circumstances, such as voice commands in Thai and English via Wi-Fi, 4G, and 5G internet connectivity. The experimental investigation can determine, construct, and assess a smart home automation system that operates on IoT devices, specifically focusing on lighting control and intrusion detection. The authors propose a novel matric factor of critical system efficiency and responsiveness to ensure the system can sustainably support voice commands for light controls, intrusion detection, home wireless networks, and evolving cellular network systems. In addition, the accuracy and responsiveness of intruder detection using PIR

sensors based on varying delay detection times are investigated. Thus, the study addresses the following fundamental research questions:

- How can the hardware and software components of an IoT-based smart home system be integrated to ensure seamless communication and cooperation between home automation, intruder detection, and lighting control functions?
- How is the extent of the proposed framework effective in achieving smart lighting control? Consider factors of system effectiveness related to response time, accuracy, and internet connection performances in the context of voice and motion detection on various internet connections.
- How do IoT-based smart home systems affect the accuracy of intruder detection on various PIR delay detection times?

By focusing on combining home automation and intrusion detection using voice commands, the results of this research contribute to the design and development of an IoT-based framework, hardware, and processes, and assess the system accuracy and responsive performances of various multilanguage commands on internet connections, including Wi-Fi, 4G, and 5G relating to the delay time settings of PIR sensor detection. The study recognizes the transformative potential of 5G networks to guarantee that an IoT-enabled smart home system operates accurately. By expanding on our previous study, this study explores the extended domain of 5G to comprehend how emerging cellular technology can impact the accuracy, efficiency, dependability, and user responsiveness of the proposed IoT-powered smart home automation and security system. The integration of 5G networks ensures increased data transfer speeds and enables a more precise response time for an ecosystem of interconnected IoT smart home devices. The proposed IoT-based smart home integration utilizing Raspberry Pi 4 can revolutionize human life in the fast-paced digital age of hectic schedules and expand responsibilities for the home, allowing us to create smart, responsive, and secure living environments, improving people's daily lives.

2. Theoretical Background

2.1. Emergence of Smart Home Automation System

Smart home automation systems have utilized innovative methods to improve domestic environments' connectivity, efficiency, and adaptability. The ability of users to remotely monitor and control IoT-connected devices through specialized applications provides an exceptional level of flexibility, enabling home management regardless of the user's geographical location [30,31]. Smart home security refers to a range of devices specifically designed to improve the safety and protection of residential areas. These devices include smart cameras, doorbells, locks, sensors, alarms, atmosphere control, and network security measures. Several prior studies have suggested smart home automation systems in diverse domains. Satapathy et al. [32] introduced a novel and economical home automation system utilizing the Arduino framework, which offers straightforward Wi-Fi Internet connectivity. This configuration allows users to access and control their electric devices using smartphones remotely. The essential hardware components consist of an LCD, a relay, an Arduino module, and an ESP8266 in the hardware configuration. Their experimental configuration is meticulously calibrated to optimize the control of diverse domestic devices and proudly exhibits a remarkable efficiency rate of 100 percent. Sharif et al. [33] introduced an innovative home automation model based on the layouts of residential units as part of a simultaneous endeavor. This model offers exceptional versatility in choosing hardware, devices, and communication protocols. The design streamlines essential elements of home automation, particularly the security functionalities. The proposed model provides detailed technical specifications for the hardware and software components of home automation systems. A notable apprehension is that the development process depends exclusively on open-source and readily available software technologies. This strategy enhances the system's flexibility and prepares it for deployment in diverse real-world situations. In their study, Stolojescu-Crisan et al. [34] introduced qToggle, an innovative system that connects sensors, actuators, and various other data sources. The system facilitates smooth communication by

harnessing the capabilities and flexibility of an application programming interface (API). The qToggle APIs are commonly executed through sensors and actuators with network connectivity in the upstream direction. Most qToggle devices utilize ESP8266/ESP8285 chips or Raspberry Pi boards. A specialized smartphone application has been created to enhance user accessibility and control by allowing the remote management of a wide range of home appliances and sensors. These three methods demonstrate the ever-changing field of home automation and emphasize the various strategies used to simplify and enhance the control of household environments. These systems enable the development of smart home technology solutions that are more efficient, cost-effective, and flexible, thanks to innovative hardware and software configurations.

The smart home automation system has been researched to enhance home management and convenience in various aspects, including responsiveness, accuracy, and voice command integration [35,36]. The instantaneous execution of commands and adjustments is essential for ensuring security features and energy management. Precision is the primary objective of accuracy, aiming to carry out tasks with minimal errors to foster user confidence. A previous study includes regulating temperatures, controlling lights, and managing intruders. The implementation of voice command technology can be customized to enhance user-friendliness via the control system [19,37]. The system provides unmatched convenience and accessibility, enabling users to control various aspects through voice commands. The voice command functionality can be practical, particularly for individuals with mobility limitations or visual impairments [29]. Smart home automation systems benefit from quick responsiveness, precise accuracy, and easy-to-use voice command capabilities, improving efficiency, comfort, and accessibility [35]. Dbritto et al. [38] and Zaro et al. [39] examined the utilization of Wi-Fi and mobile applications for the purpose of control and monitoring. Zaro et al. [39] also highlighted explicitly the use of Arduino technology to achieve cost-effectiveness.

Communication technologies, such as 3G, 4G, and 5G, play a pivotal role in the efficient functioning of smart home automation systems [29,40,41]. These cellular connections are important and essential for facilitating effective communication between diverse devices and systems. They ensure universal compatibility across different network generations and maintain the functionality of smart home devices in various network environments. The evolution of cellular networks from 3G to the more advanced 4G and 5G networks signifies a significant leap in enhancing the effectiveness of smart home automation systems. However, it is important to note that while these technologies can significantly enhance the functionality of smart home systems, they may make the systems more complex and expensive to install and use. Many smart home systems are designed to be user-friendly and cost-effective, making them a practical choice for homeowners. The interconnected nature of smart home devices heavily depends on data speed and capacity for real-time data transmission and processing. The advent of 5G technology significantly reduces latency, which is vital for smart home applications that require immediate responses, such as security systems. It also boosts smart home automation systems' reliability, efficiency, and responsiveness [35,41–43].

2.2. PIR (Motion) Sensors for Intruder Detection and Security

Afreen et al. [44] introduced an innovative smart surveillance system designed for security areas using an IoT framework and a gravity microwave sensor. The Arduino UNO is utilized to control the operations of this setup. The system rapidly transmits a real-time alert message when a sensor, utilizing microwaves within its designated coverage area, detects object movement. The system uses a GSM module to establish a call connection to a cloud service. While a gravity microwave sensor remains unaffected by environmental factors such as temperature fluctuations, it necessitates precise placement to achieve optimal accuracy in larger areas. On the other hand, a PIR sensor is particularly adept at detecting motion in specific regions, making it ideal for intrusion detection purposes. Combining a Raspberry Pi with a PIR sensor creates an intrusion detection and alarm system. This

system can include a siren for immediate alerts and the ability to send email notifications to the administrator in the specified area. The PIR sensor is commonly and exceptionally well suited to motion detection, given the characteristics of its infrared waves. In order to precisely detect human and animal motions, electronic security systems frequently implement PIR sensors; however, despite their relatively low cost, false positive alarms may still happen on IoT-enabled PIR systems due to sudden environmental fluctuations, such as altitude, height, light, temperature, and angle [20].

In addition, positioning and calibration accuracy are crucial to achieve optimal performance. Implementing PIR sensor technology is routine in intrusion detection and action movement systems [45,46]. When combined with additional security protocols, the sensors provide enhanced protection for residential properties, commercial establishments, and places of business [47]. Nevertheless, implementing these technologies poses difficulties when attempting to reduce false alarms and ensure precise detection. Design and development are essential during the design and installation of a system to meticulously evaluate environmental factors, such as temperature fluctuations, as they can affect the functionality of sensors. PIR sensors are also commonly utilized for reliable and economical intrusion detection [45]. Difficulties arise due to the environment's delicate characteristics and the requirement for accurate calibration. In order to maximize the potential of PIR sensor technology for enhancing security and automation systems, this study seeks to assess its practical capabilities.

2.3. Voice Recognition in Smart Home Security

Currently, the automated smart home system adapted to voice command recognition is an essential technological element along with smart home security systems, providing a convenient and secure method to manage different home devices [48–50]. Gunawan et al. [51] and Wang [52] emphasized the significance of precise speech recognition in these systems. In addition, Gunawan [51] showcased the efficacy of the cloud speech technique by employing the Google Voice Kit to enhance processing speed and accuracy. Abidi et al. [49] and Chenxuan [50] highlighted the potential of voice control in augmenting home security, specifically in improving user experience and accessibility. Abidi et al. [49] emphasized the utilization of vocal commands for the management of household devices. Chenxuan [50] investigated a tailored speech recognition system designed specifically for elderly individuals.

Furthermore, the mobile version of Google Translate is a potent instrument that surpasses linguistic obstacles through its voice recognition system. The Google Translate framework can facilitate a collaborative multimodal communication experience by offering instantaneous translations in more than 100 languages and offline translations in almost 60 languages [53]. Incorporating voice recognition technology has enhanced Google Translate's proficiency in natural language processing (NLP). The framework comprehends the subtleties of verbal communication, including accents, intonations, and colloquial expressions. These facilitate the acceptance of various inputs through users' typing, speaking, or utilizing the camera translation feature. Several studies have investigated the use of Google Translate voice recognition in multiple applications. Wang [52] effectively employed Google Cloud's speech-to-text and translation services for video translation, despite encountering difficulties with loud background music and literal translation. Lee et al. [54] integrated facial and vocal recognition into a smart home security system, utilizing a Raspberry Pi as the central component and attaining enhanced convenience and security. Ali et al. [55] implemented an IoT security system with voice recognition. The system incorporates intelligent personal assistant (IPA) systems integrated with the Google speech-to-text API. The simulation results indicate that the system has a high level of proficiency in recognizing 90% of the device names linked to all commands and achieving a 100% accuracy rate in correctly classifying commands within an approximate time frame of 30 s.

2.4. Overview on Thai Users and Thai Language

Thai culture is a diverse and intricate fabric of traditions, values, and customs that shape the way of life for its people, in clear opposition to Western culture. Culture significantly influences Thai individuals' perceptions and subjective responses, particularly in situations involving voice quality tests, despite the broad and non-technical nature of the term 'culture'. This phenomenon illuminates the overall impact of cultural diversity on individual assessments. The Thai language is integral to Thai culture, serving as the primary mode of communication in the country. Thai is a tonal language with five distinct tones, one of which is also found in Chinese and Vietnamese. The remarkable nature of the Thai language lies in the significance of its tone and pitch changes within its linguistic structure. The slight deviations in tone are not insignificant details; they are essential components of language that can modify the definitions of words and phrases [56,57]. The Thai language holds significance in this context, surpassing its unique linguistic traits. The Thai tonality is a captivating example of linguistic diversity's broader challenges and possibilities. The intricate tonal variations in the Thai language highlight the importance of being aware of and respectful of the cultural and linguistic subtleties present in communication, particularly in diverse and multilingual environments. The Thai language is an exemplary case study highlighting the intricacies involved in cross-cultural communication when examining subjective evaluations, such as voice quality assessments. The importance of cultural and linguistic diversity in assessing responses to voice commands is emphasized in this study. The following are some examples:

Mid-tone	ปา (pa)	means	to throw
Low tone	ป่า (pàai)	means	forest
Falling tone	ป้า (pâai)	means	aunt
High tone	ปึ๊ (páp)	means	father, daddy
Rising tone	ป๋า (pă)	means	father, daddy

The intricate tonal system of the Thai language may pose a challenge for individual learning, especially for Western people, to comprehend and practice. Thai tone marks may be more complex to learn clearly and quickly than in Western languages. The emphasis on tonal aspects in Thai linguistics makes the subject more comprehensible and feasible for sentences and actions. The distinguishing characteristic of the Thai language is its simplified grammar. In the Thai language, neither the definite "the" nor indefinite "a", "an" articles, which are commonly employed in English, are applied. So, a Thai sentence is an exclusion function to simplify communication. Thai further streamlines the use of object pronouns, verb conjugation, and noun declension. In Thai, the verb "to be" remains constant regardless of the subject, unlike in English, where it varies as "is", "am", or "are". Furthermore, it does not necessitate conjugations or modifiers to ensure agreement between subject and verb, number, tense, or gender. Furthermore, this facilitates the acquisition of knowledge and establishes Thai as an independent linguistic entity.

The processing of the Thai language poses challenges, particularly concerning identifying phrase boundaries and sentence markers. Thai creatively employs whitespace, in contrast to Western languages. It visually and conceptually separates words, phrases, and sentences; many languages require improvement. The Thai phrase for "I love you" is written as "I-love-you" without any inter-linear spaces, which can perplex individuals from Western cultures.

Give thought to the English expression "God is nowhere". Spacing and structure would substantially modify the clarity and interpretation of the phrase in Thai. This instance highlights how the Thai language, characterized by its distinct syntax and structure, provides a unique linguistic encounter, distinguishing it from the diverse global languages. Like its English counterpart, this Thai term can have various interpretations such as "God is not where", "God is nowhere", or "God is now here". The different meanings depend on the context, showcasing the contextual adaptability inherent in the Thai language [57]. The linguistic idiosyncrasies highlight the intricate nature of Thai and its distinctiveness when compared to Western languages. Although Westerners may find it difficult to learn

Thai tones, its simplified syntax offers a striking juxtaposition. The lack of certain linguistic elements, such as articles and complex conjugations, emphasizes the Thai language's distinctive features. Thai language requires a nuanced understanding and appreciation, especially for speakers of Western languages.

3. Materials and Methods

Section 3 of this article provides an in-depth analysis of the operational and design components of our novel IoT-driven smart home automation and security system. This segment has been carefully structured to optimize logical progression and comprehension by methodically dissecting the intricate elements of our system. Section 3.2 provides a primer to the comprehensive framework of our IoT-based smart home security architecture solution, elucidating its interconnectedness and stratified arrangement. Section 3.3 establishes the groundwork for a comprehensive examination of the hardware and system design, clarifying the functions of every element comprising the IoT smart home security ecosystem. Section 3.4 describes our experimental configuration and method of data collection, illustrating how our system was evaluated in real-world scenarios. Every subsection is interrelated, building upon the preceding one in order to furnish a thorough comprehension of the architecture, components, and performance evaluation of our system.

3.1. Research Methodology

This study aims to implement an IoT-based smart home automation system efficiently to detect intrusions and notify a user using lights and buzzers. The Raspberry Pi 4 can be utilized in conjunction with voice commands. This study includes two primary empirical investigations. The fundamental objective of the experiment is to consistently evaluate the system's accuracy and responsiveness in common user-controlled scenarios, such as switching lights on and off and establishing internet connections via Wi-Fi, 4G, and 5G networks. Another objective is to assess the accuracy of intruder detection. This evaluation zeroes in on the system's performance in scenarios involving intruder detection, specifically scrutinizing the response times of the PIR setting. These response times are categorized as low (5 s), medium (2.5 s), and high (1 s). This exhaustive evaluation aims to foster confidence in the audience about the system's capabilities.

Assessing various PIR delay time settings in the IoT-based smart home system is essential for comprehending the system's performance in different situations along with communication protocols. This study rigorously analyzed the performance of the PIR sensor, specifically emphasizing its ability to detect intruders, even when no people are present promptly. The significance of this evaluation lies in its capacity to uncover the functional characteristics of the system and its potential for improvement, particularly in applications.

To mimic real-life conditions for the secondary objective, a PIR sensor is strategically placed in front of the testing area at a height of 1.8 m, adhering to the recommended guidelines for PIR sensor installation [37]. During the system's testing phase, data are collected from three distinct sources: Thai speech, English speech, and the control buttons of the Blynk mobile application. Each experimental scenario is repeated 100 times, demonstrating our rigorous approach to data collection. This thorough method ensures a comprehensive evaluation of the proposed intrusion detection and smart lighting control system that leverages the IoT. The resulting system lays the groundwork for understanding the capabilities and limitations of the developed system in practical situations.

3.2. Design of IoT-Based Smart Home Framework

The design of the IoT framework makes a substantial contribution to the domains of home automation and security, as demonstrated in this study. Integrating multiple technological aspectual components and layers [12,16,58], and encompassing user interface applications and physical hardware, the framework offers a comprehensive approach to smart home solutions. The IoT-based smart home framework introduces a groundbreaking

multilayered approach, drawing inspiration from various system design domains. This innovative method enhances user interaction with the system, employing fresh techniques for user engagement. Unlike previous models, the framework uniquely integrates aspectual layering components, offering more modular and replaceable parts. The proposed design leads to more straightforward upgrades and maintenance, and showcases a unique ability to adapt to emerging technologies, such as the latest generations of network connectivity like 5G communication technology. The framework's security features, particularly the inclusion of PIR sensors and real-time alert systems, are more advanced and integrated uniquely compared to previous systems.

The smart home environment's interpretation and processing of user commands and sensor data necessitate a range of sensors and commands with a responsive and accurate methodology. Integrating multilayering semantics adaptation in services has significantly enhanced our framework's design. Each framework layer operates independently by employing this strategy while integrating seamlessly, ensuring smooth operation and intuitive user engagement. This innovative adaptation boosts the system's responsiveness and enhances its ability to learn and adapt to the homeowner's habits and preferences over time. This integration establishes a comprehensive system that simplifies home automation and security management, incorporates sustainability principles and quality assessment mechanisms, and enhances user interaction and knowledge capabilities. Combining these diverse components from various fields results in an innovative and potentially transformative IoT smart home design methodology.

The system's architecture enables real-time control and monitoring, essential for improving a smart home's security, comfort, and energy efficiency. Incorporating well-known platforms and protocols, such as Google Assistant for voice control and MQTT for communication, demonstrates the adaptability and future compatibility of the IoT-enabled system with evolving smart homes.

The IoT-based smart home framework, illustrated in Figure 1, is a meticulously engineered and stratified system that provides a comprehensive approach to safeguarding residential premises. The framework is composed of hardware, software, and applications, which are all distinct layers. Each layer is composed of a multitude of components that work in conjunction to establish a secure and efficient smart home environment.

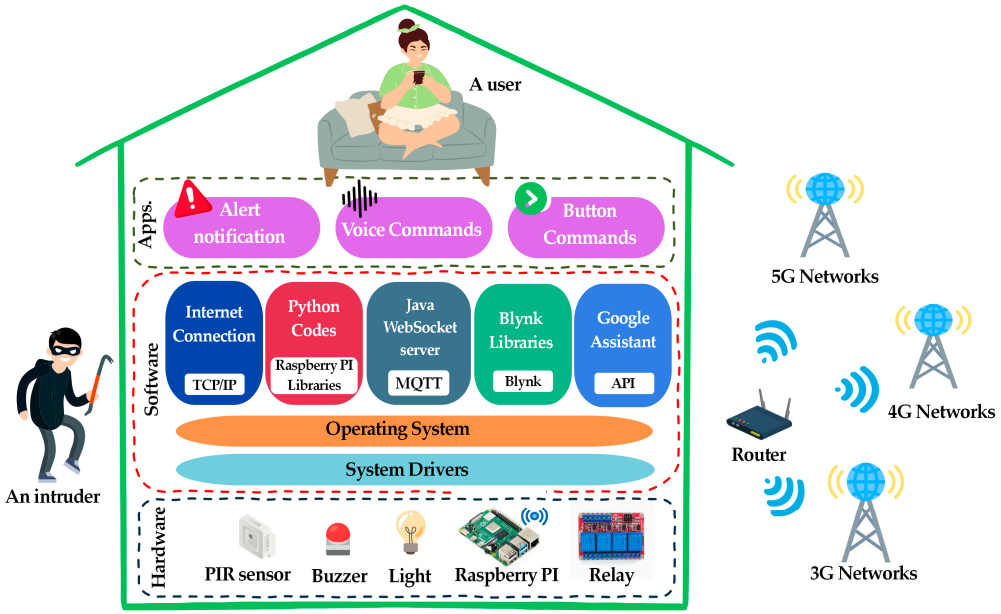

Figure 1. IoT-based smart home framework using the PIR intruder detection system.

Physical elements such as PIR sensors, buzzers, lights, a Raspberry Pi, and a relay comprise the foundational level. These devices are of the utmost importance as they function as the central control unit (Raspberry Pi) that processes input from various sensors and generates signals to execute actions such as activating lights or triggering alarms, in addition to detecting intrusions via the PIR sensor and issuing alerts via buzzers and lights.

The software layer functions as an intermediary, facilitating the conversion of hardware signals to executable data, situated superior to the hardware and vice versa. The Raspberry Pi software package consists of various software components, including the operating system and system drivers. The elements as mentioned earlier comprise Internet connection protocols (TCP/IP), coding libraries for Python and Java, a WebSocket server facilitating real-time communication, MQTT enabling lightweight messaging, and application programming interfaces (APIs) integrating with smart devices and enabling voice command capabilities, as exemplified by Blynk and Google Assistant.

The user interacts with the system at the highest layer. The system consists of user-friendly interfaces and applications that deliver notifications and enable voice and button commands for system management and control. The visual presentation and user interaction are the responsibility of the user interface layer, irrespective of the user's location or remote access to the system via Wi-Fi, 4G, or 5G networks.

By compartmentalizing functionalities into discrete layers, the IoT-based framework offers many advantages. This layering methodology allows for flexibility in selecting and integrating various components, ensuring the system's adaptability to evolving technologies. It also promotes compatibility between different devices and services, facilitating seamless integration. Moreover, the layered structure enables accurate configuration, allowing for comprehensive adjustments and calibrations at every tier, promising precise reactions to security threats, and optimizing the performance of smart home automation functionalities.

The flexibility of the IoT framework has been intentionally engineered to accommodate the rapidly advancing domain of smart home technology. From the physical hardware to the user interface, the structural layers can be subdivided into numerous layers, allowing for the autonomous updating or replacement of each segment in response to the emergence of more advanced technologies. This IoT-enabled home automation and security system is designed with user-friendliness and seamless integration. Utilizing widely recognized communication protocols such as TCP/IP and MQTT guarantees seamless connectivity with many devices and services.

The system can effortlessly adapt to evolving requirements or emerging technologies by updating or substituting specific layers or components—all without requiring a comprehensive system redesign. The implementation of the layering methodology provides the advantage of flexibility in selecting software and hardware components. The framework is illustrated by the smooth incorporation of an innovative sensor into the hardware layer, which has no observable impact on the software or applications layers.

Every successive layer functions as a modular interface, guaranteeing compatibility between various components and technologies. The capability to establish standardized communication protocols that ensure compatibility with a wide variety of multiple application interfaces and hardware devices is implicit in the software layer. A layered framework facilitates the configuration procedure during implementation. These framework features enable comprehensive adjustments and calibrations at every tier, promising precise reactions to security threats and optimizing the performance of smart home automation functionalities. Compatibility with the system is extensive and wide-ranging, extending from primitive sensors to intricate sensors along with cloud-based platforms.

3.3. Hardware and System Design

The practical system under investigation includes Wi-Fi connectivity tested within a smart home environment, while scenarios involving 4G and 5G mobile connections were tested outdoors. The results illustrate the system's agility in enabling remote access and the control of electrical devices through smartphones. The system is precisely engineered to

automate lighting control and enhance security, utilizing motion detection to activate lights or alarms. The system's functionality relies on the precise programming of a microcontroller board built on a Raspberry PI. This microcontroller board processes the input from the PIR sensors and manages the output to the lights and buzzers through the relay module, as depicted in Table 1.

Table 1. Hardware and system components for the IoT-based smart home security framework.

Type	Component	Description
Hardware	Light Lamps (240 V)	The relay module controls and most likely activates these devices in response to different triggers.
	Relay AC 240 V 12 V	Relay modules function as switches, enabling low-voltage circuits to regulate high-voltage lamps.
	PIR (Motion) Sensors	PIR sensors detect motion by detecting alterations in infrared light, which subsequently activate other actions.
	Buzzers (#1 and #2)	Devices that produce an audible sound upon activation are likely employed for security notifications.
	USB Micro-B	Supplies power or facilitates the connection for programming the control board.
	Microcontroller Board	The central processing unit executes the control software, most likely a Raspberry Pi.
System	Operating System	The microcontroller is typically equipped with a Linux-based operating system for Raspberry Pi.
	Control Software	Software applications or scripts developed in programming languages such as Python or C++ or utilizing platforms like Node-RED are responsible for handling the relay and sensor inputs. These applications constantly monitor the inputs from the PIR sensors and issue commands to the relay module to control the lamps and buzzers.
	Drivers	Software interfaces facilitate the interaction between control software and hardware components, such as GPIO pins.
	Scheduling/Event Management	The software's logic processes events using conditional triggers such as time or sensor input.
	Networking Software	Components for remote control and notification may involve the integration of web servers or IoT communication protocols, such as MQTT, to enable remote control and notification functionalities.

Figure 2 illustrates the visual structure of a smart home security automation system. The incorporation of vital elements guarantees a unified and adaptable structure. The system consists of a Raspberry PI that facilitates communication and interaction between a relay, PIR sensors, light lamps, buzzers, and a USB micro-B connection. The integration of these components creates a smart home security automation system that is responsive and adaptable, effectively utilizing technology to protect and improve the security of the home environment.

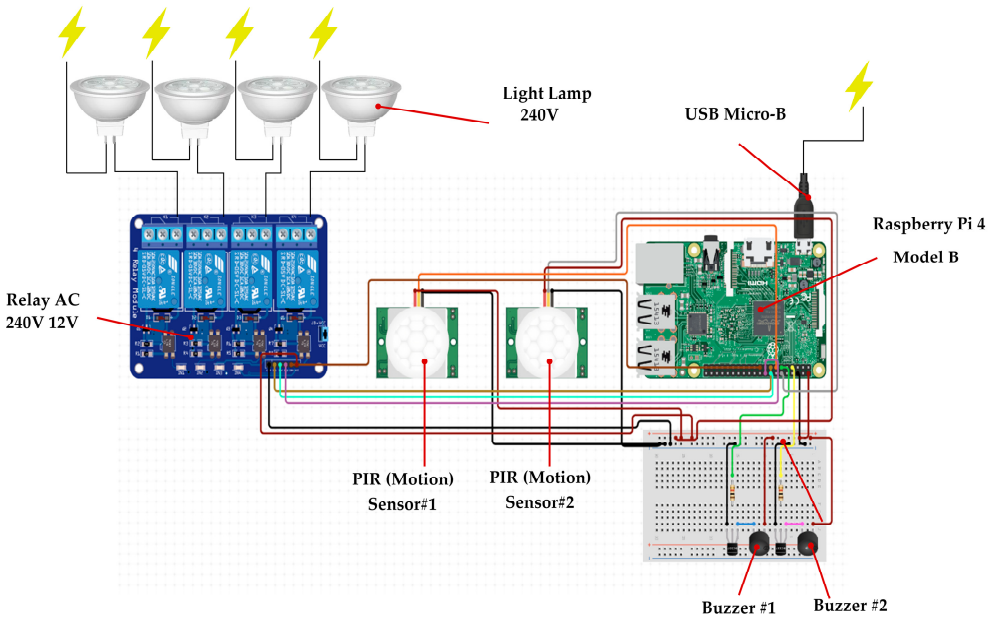

Figure 2. System architecture of the IoT-driven smart light control and intruder detection.

The proposed smart home security and automation system utilizes a seven-step algorithm that combines IoT technology with user-friendly interfaces, as depicted in Figure 3. The system algorithm comprises the following:

- System activation: The process begins by supplying power to the Raspberry Pi 4, which functions as the central control unit for the system.
- PIR sensor surveillance: The system utilizes PIR sensors to detect motion. Upon detecting motion, the system promptly triggers the buzzer and illuminates the lights as an instant security measure.
- Relay status verification: When no motion is detected, the system verifies the status of the relay. When the relay is activated, the lights stay illuminated; when deactivated, the lights are switched off to conserve energy.
- The system actively listens for voice commands, simultaneously prepared to interpret instructions from the user.
- Voice command authentication: When a voice command is received, the system verifies its authenticity to decide whether to activate or deactivate the lights.
- Command execution: The system performs the command by activating the relay to switch the lights on or off, demonstrating the system's ability to respond promptly to automated sensor inputs and user commands.
- System reset: After actioning any command, the system resets to its original state, ready to detect new motions or receive further voice commands.

In this study, the synthesis steps enhance security through efficient intruder detection and provide convenience for remote lighting and alarm control as follows:

- Enhanced security: The immediate activation of buzzers and lights upon motion detection by the PIR sensors deters potential intruders and alerts the user.
- Remote control: Users can control lighting and alarms remotely via the Blynk application or voice commands through Google Assistant.
- User notifications: The system notifies the user of detected intrusions, allowing for the quick deactivation of alerts if necessary.
- Multilingual support: With support for both Thai and English, the system caters to a diverse user base.

- Protocol utilization: The use of MQTT and IFTTT protocols enables smooth integration with various devices and services, making the system adaptable to a wide range of scenarios.
- User-centric design: The system's design considers the user's importance, conveniences, and needs in smart home solutions on responsive control and usability.

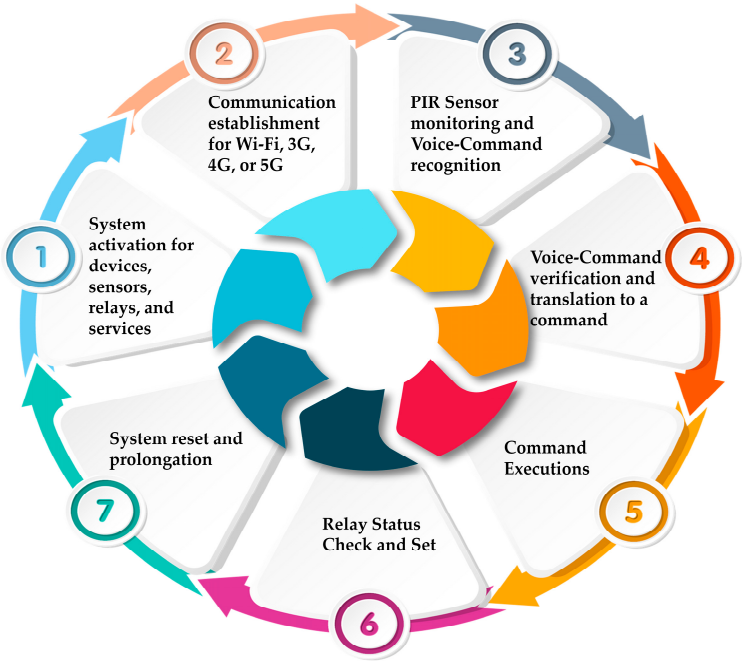

Figure 3. A process of seven-step operations designed for the IoT-based smart home and PIR intruder detection system.

3.4. Experimental Setup and Data Collection

This study examines an IoT-based smart home automation system centered on intrusion detection and lighting control using a Raspberry Pi 4. The setup includes PIR sensors for motion detection and an array of smart devices for lighting, operating over Wi-Fi, 4G, and 5G networks to assess performance across diverse connectivity scenarios. Data collection is a hybrid of automated processes using Google Assistant and manual processes using user inputs. The voice-activated assistants interact with Raspberry Pi 4 devices using the MQTT and IFTTT protocols. These protocols are essential for converting spoken commands into electronic signals, allowing users to control the system with their voices. The manual processes capture system responses to Thai and English voice commands and inputs from the Blynk, alongside manual recordings by the authors for comprehensive analysis. The proposed IoT-based system incorporates PIR sensors for intrusion detection based on area. PIR sensors have a specific detection range and angle limitations based on [20]. This research employs two sensors to collectively cover a more extensive detection range and a variety of angles, thereby improving the system's detection capabilities.

Upon detecting an intruder within the range of PIR sensors, the system immediately activates the corresponding light bulb and initiates a buzzer system to notify the user promptly. The Blynk application has the capability to turn off the light and buzzer for the sake of convenience. The system initialization commences with activating the relay located in the adjacent state. Both the Blynk application and Google Assistant can manually activate the light. The system, equipped with PIR sensors, operates as a multitasking device and maintains constant vigilance for intruders. When the system detects an object in its field of view, it promptly triggers the light and buzzer while also displaying a notification that says, "An intruder has been detected". The user retains control via the Google Assistant application and can promptly deactivate the light and buzzer. The

system integrates IoT technology, voice recognition, motion detection, and user-friendly interfaces. The system's main advantage lies in its heightened security through intruder detection and the convenience of remotely controlling lighting and alarms using user-friendly smartphone applications. Furthermore, its ability to function effectively in Thai and English and its compatibility with MQTT and IFTTT protocols showcase its versatility in diverse practical scenarios.

This study examines the precision of intruder detection using different PIR sensor detections. It introduces two metrics: average effectiveness response time (AERT), which measures the time it takes for the system to respond after a command is issued, and average accurate intruder detection (AAID), which evaluates the system's accuracy in detecting intrusions. The data sampling strategy is systematically designed to capture a wide range of system performances, with regular intervals and customization based on the experiment's characteristics. To replicate real-life usage scenarios, an experimental investigation is carried out under diverse conditions, encompassing varying time periods throughout the day and network environments. The entirety of the data are systematically documented and stored within specialized IoT data management systems. Prior to analysis, the data undergo meticulous preprocessing procedures such as cleaning and normalization to ensure precise results. In order to guarantee the trustworthiness and accuracy of the data, every experimental scenario is duplicated numerous times, frequently reaching up to 100 repetitions. This process establishes a strong basis for assessing the effectiveness and flexibility of the system in different circumstances and with various inputs.

4. Results and Discussion

Emphasizing user-centric design, this study offers a sophisticated approach to home automation, promising increased convenience, efficiency, and security, and thus contributing substantially to the evolution of a solution using an IoT-based smart home framework. The proposed framework marks a notable advancement in the IoT-based smart home security domain. It demonstrates a significant improvement in voice command recognition, particularly for adapting multilanguage commands, indicating a leap in language processing effectiveness. The system shows impressive adaptability across various network technologies, especially in integrating the emerging 5G communication technology, aligning it with current global technological trends. This study also highlights the precise detection capabilities of PIR sensors, suggesting configuration settings that enhanced real-time security monitoring. Furthermore, the in-depth evaluation of system responsiveness across different conditions underscores its operational efficiency.

This experiment thoroughly investigated a system-controlled smart lighting and detection system, analyzing its performance in various scenarios, including manufacturing variations, extended usage, and changes in manufacturing techniques. The characteristics of the PIR detector can influence the system's operational efficiency. This study found the comparison of detection capabilities among detectors deployed in the same environment but configured with different delay detection responses to be particularly intriguing. This study methodically categorized testing conditions into three groups according to the levels of delay: low, medium, and high. These experiment approaches were made using two different methodologies called Blynk and Google Assistant. Every method was thoroughly assessed through 100 iterations to evaluate response times in four communication modes: direct, 4G (300 Mbps), 5G (1 Gbps), and Wi-Fi (866 Mbps). Therefore, each experiment's average effective response time was calculated with great attention to detail, providing valuable insights into the system's performance under different circumstances. This study precisely determined the detector's coverage area by specifying a height of 180 cm and a reach of up to 700 cm, as indicated in reference [20]. This configuration facilitated the evaluation of the latency of Blynk button commands and Google Assistant voice commands. The response time of the Blynk application relied heavily on the system's capacity to detect an intruder entering the equipped room or effectively execute commands to control the

system-controlled lights. The primary objective of the investigation was to clarify the intricacies of response times across various communication modes.

Table 2 displays the outcomes of the experiments that aimed to assess the efficiency of the IoT-based smart home system in different network scenarios, such as 4G, 5G, and Wi-Fi. The system employed Blynk button commands and Google Assistant in Thai and English. Concerning the commands "Turn on light" and "Turn off light", the system exhibited satisfactory performance, with a consistently low average error rate time (AERT) ranging from 2.4 to 5.3 s under different network conditions and voice assistant platforms. The English voice assistant had an 18% failure rate in activating the lights. The system's commendable accuracy was demonstrated through intruder detection scenarios using AAID. The system consistently attained AAID scores within the range of 2.2 to 4.7 in scenarios characterized by low response times of 1 s. The AAID results showcase the system's capacity to promptly and precisely identify trespassers in real time. In situations where the response times were moderate (2.5 s), the system consistently demonstrated high accuracy, as indicated by AAID scores ranging from 2.7 to 5.6. The precise identification of intruders showcases the system's dependability in promptly detecting unauthorized individuals with a delay of only 2.5 s. Despite a 5 s delay, the system's AAID scores ranged from 5.8 to 7.5 in intrusion detection scenarios, indicating its accuracy in detecting intruders. The IoT-based smart home system successfully detected intruders, even under fluctuating network conditions and response times, as depicted in Figure 4. Nevertheless, there were occasional problems executing voice commands, specifically when utilizing the English voice assistant. To enhance the overall reliability and responsiveness of the system, it is essential to analyze these occasional failures and make necessary adjustments.

Table 2. Comparing responsive and accurate results for voice commands of lighting controls.

Experiments	AERT (s) of Blynk Voice-Button Commands				AERT (s) of Google Assistant (Thai)				AERT (s) of Google Assistant (English)			
	5G	4G	Wi-Fi	Fails	5G	4G	Wi-Fi	Fails	5G	4G	Wi-Fi	Fails
Turn on light	4.8	5.3	2.4	0	3.7	4.5	3.9	18	3.2	4.7	4.2	9
Turn off light	4.8	5.3	2.4	0	3.6	4.5	3.9	16	3.2	4.7	4.2	8
Turn security on	3.5	4.3	2.6	0	3.7	4.7	4	17	3.4	4.9	4.3	10
Turn security off	3.5	4.3	2.6	0	3.7	4.7	4	18	3.4	4.9	4.3	9
PIR detection response with low delay (1 s) AAID	2.7	3.1	2.2	0	4.7	4.8	4.1	0	4.7	4.9	4.1	0
PIR detection response with medium delay (2.5 s) AAID	2.7	4.2	2.9	0	4.9	5.6	5.3	0	4.9	5.7	5.3	0
PIR detection response with high delay (5 s) AAID	6.4	7.4	5.8	0	6.8	7.4	5.9	0	6.8	7.5	5.9	0

Figure 4 depicts the performance of different commands carried out through different network connections (Wi-Fi, 4G, 5G) in three experimental configurations: Google Assistant voice commands in English, Google Assistant in Thai, and Blynk button commands. The commands encompass PIR detection with adjustable delays and operations for managing security and lighting. The execution of "Turn off light" commands was nearly flawless in all scenarios, demonstrating high performance. Instructions to "Disable security" were also highly effective, although with slightly lower implementation rates in Thai voice assistance. The PIR detection commands correlated with the delay's duration, whereby shorter delays resulted in improved execution. However, these commands were still less effective than the light and security ones. The shift from Wi-Fi to 4G and subsequently to 5G led to decreased command failures, especially in voice assistance experiments. This result indicates that newer network technologies can improve the reliability of command execution. Moreover, voice commands in Thai encountered slightly more significant obstacles in their implementation than in English, indicating possible difficulties in language processing. To summarize,

the data indicate that both network technology and command type impact performance. However, overall, there is a high success rate in executing commands, particularly when using 5G connectivity and commands that do not experience delays or time-related issues.

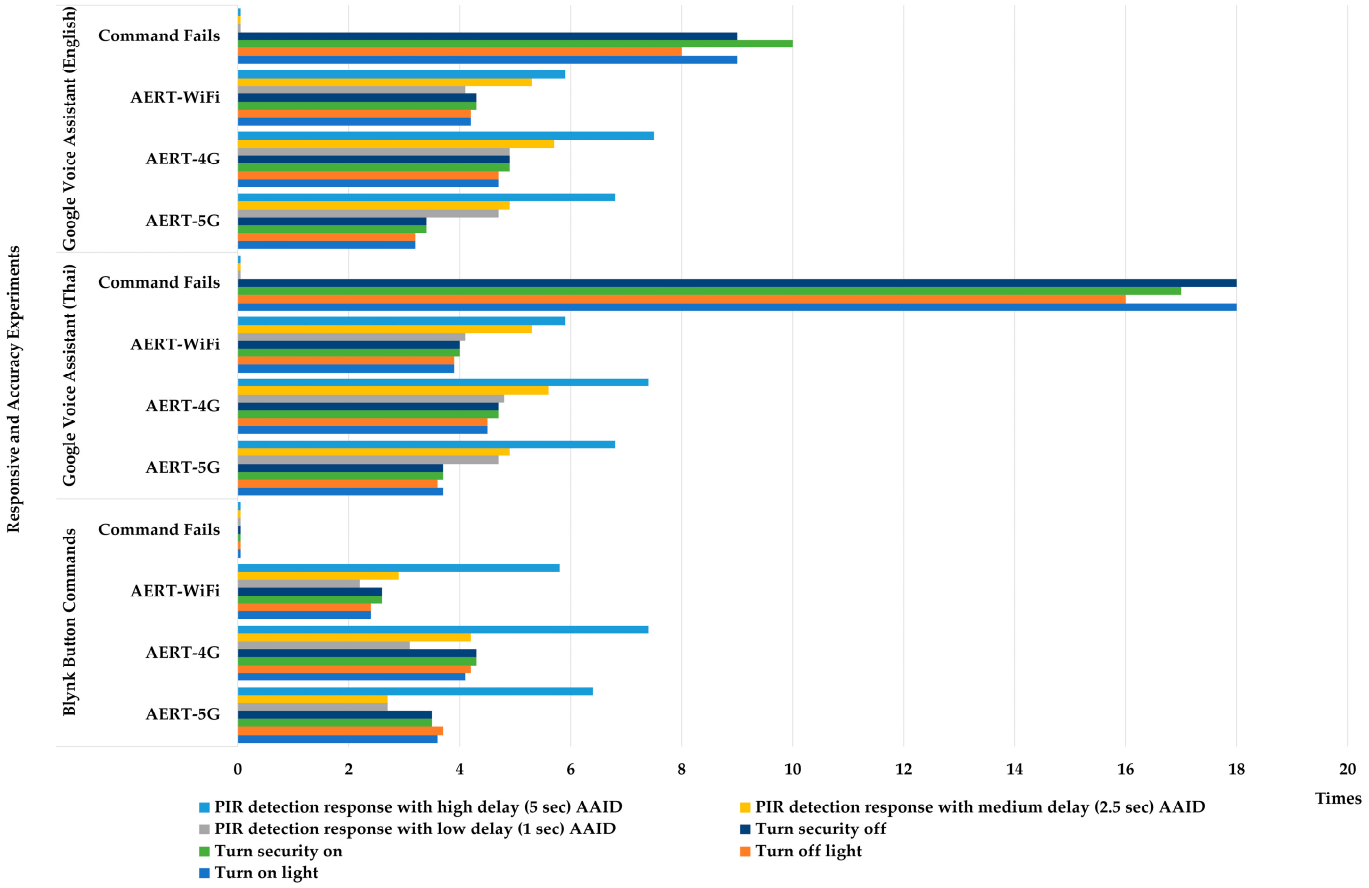

Figure 4. Comparing responsive and accurate commands of PIR intruder detection and lighting control on various connections.

The experiments revealed that the system's ability to promptly respond to the "Set alarm on" command, regardless of the type of network connection, is a noteworthy discovery. The result in Table 3 demonstrates button-command responsiveness and accurate results for intruder detection. The data table displays the outcomes of different Blynk notification experiments, including metrics for command execution on 4G, 5G, and Wi-Fi networks, as well as detection failures at different times of the day. The prompt occurrence of alarms upon receiving instructions was evidenced by the low AERT of button commands across various communication networks. It performed admirably regarding 4G, 5G, and Wi-Fi networks, respectively.

This finding holds considerable importance for real-world security applications, as it guarantees the prompt activation of alarm systems in reaction to potential intruders or security threats. This feature showcases the system's reliability in promptly executing crucial user instructions, enhancing its effectiveness as an intelligent security solution. The primary conclusions derived from this dataset are as follows:

- PIR detection with low and medium delays, as well as commands to turn on and off alarms, achieves a flawless success rate throughout the entire day, without any failed detection in the morning, midday, evening, or at night.
- AERT-Wi-Fi typically provides the quickest response times for turning alarms on and off and for PIR detection with low to medium delays, followed by AERT-5G, and AERT-4G provides the most extended response times. This result may suggest that

Wi-Fi offers a more responsive connection for the aforementioned tasks in the tested environment, which contradicts the anticipated faster speeds of 5G.

- PIR detection experiences a substantial increase in response time, accompanied by a substantial delay of 5 s (AAID). This result is especially pronounced in the AERT-4G and AERT-5G setups, which have longer response times than AERT-Wi-Fi.
- For PIR detection with a high delay, there is a notable number of detection failures at all times of day, with the highest number of failures occurring at noon (22 failures), followed by evening (17 failures), night (16 failures), and morning (18 failures). This result indicates that an increase in AAID consistently negatively impacts the system's dependability over the day.
- From the data, we can deduce that while the type of network does impact the response times for commands (with Wi-Fi often outperforming 4G and 5G in this respect), the AAID set for PIR detection exerts a more significant effect on the system's reliability. Increased delays lead to a higher number of failures.

Table 3. Button-command responsiveness and accurate results for intruder detection.

Experiments	Blynk Responding Notification (s)						
	AERT			Day-Time Detection Fails			
	5G	4G	Wi-Fi	Morning	Noon	Evening	Night
Set alarm on	3.4	4.6	2.6	0	0	0	0
Set alarm off (After No movement detected)	3.8	4.8	2.9	0	0	0	0
PIR detection response with low delay (1 s) AAID	2.7	3.1	2.2	0	0	0	0
PIR detection response with medium delay (2.5 s) AAID	2.7	4.2	2.9	0	0	0	0
PIR detection response with high delay (5 s) AAID	6.4	7.4	5.8	18	22	17	16

The insights gained from the IoT-based smart home system offer essential observations about the system's responsive performance, underlining its adaptability and operational design features in various scenarios relating to wireless communication protocols and PIR delay configurations. This detailed analysis features the system's capability to manage smart lighting controls through voice activation and identifying trespassers, key aspects of home automation powered by emerging IoT technology.

This study thoroughly analyzed the PIR sensor's effectiveness in detecting intruders in real time. This study explored the sensor's sensitivity and delay configurations, uncovering its versatility and the capacity for users to customize detection settings. Users can customize the system according to their precise security requirements by modifying the delay time from one to five seconds. The empirical results demonstrated the system's adaptability, as different network communication modes, facilitated by the Blynk application and Google Assistant, impacted the system's response times.

This study revealed that delayed PIR motion detection slowdown caused the overall increase in the system's response times. This study presents comprehensive evaluations of different command types and internet wireless connection methods in the IoT-based smart lighting control system, as shown in Tables 2 and 3. The evaluated command sets include Blynk button and voice-button commands, Google Assistant in Thai, and Google Assistant in English. Significantly longer response times were observed for Google Assistant commands, particularly in English, with certain instances lasting up to 7.5 s and multiple malfunctions being recorded.

Despite these challenges, the system exhibited impressive proficiency in assessing the detection capabilities using PIR motion sensors under different response delay settings, particularly in situations with minimal response times at low delay configurations. The

findings emphasize the importance of enhancing the speed of voice command responses, especially for English commands, to boost user satisfaction and overall system performance.

Moreover, this research showcases the system's efficacy in identifying intruders using PIR motion sensors under different delay situations, accenting its dependability in security surveillance. This in-depth analysis of the workings of an IoT-enabled smart lighting control and intrusion detection system confirms the system's functionality and points out significant system components that need improvement, most markedly voice command processing and wireless network connectivity efficiency.

The system's computational complexity is a critical factor to be considered in the advanced functionalities of the IoT system, including voice command processing and real-time PIR sensor-based intruder detection. By integrating numerous sensors on Raspberry Pi 4, communication protocols, and processing units, the system's architecture is optimized to manage complex tasks efficiently. Nevertheless, the complexities associated with controlling numerous concurrent operations, particularly in extreme demand, may create considerable computational demands. The analysis reveals that the complexity of the tasks the system executes impacts its response time, which is otherwise relatively efficient. An example of this can be seen in the augmented response time for English voice commands, which indicates that language processing and interpretation require more computational resources. As a result, it is critical to maintain the system's operational effectiveness by optimizing its computational architecture to manage these complex tasks more efficiently.

Data validation and security verification are additional critical components of the system's architecture. Due to the critical nature of home security and automation systems, safeguarding data integrity and preventing unauthorized access are of the utmost importance. This study delineates the security protocols implemented by the system, which cover secure wireless communication channels and data encryption to protect against potential breaches. The PIR motion sensors and voice command interfaces are constructed with embedded security measures to ensure accurate data capture and prevent tampering. However, it is crucial to continuously adapt and update security measures to mitigate emerging threats and vulnerabilities, just as with any IoT system. The integration capability of the system with sophisticated security systems and protocols has the potential to considerably reinforce its resistance to cyber threats.

5. Conclusions

Our findings represent a significant leap in the development of IoT-based home automation systems, showcasing a functional and practical innovative system with potential real-world applications. As technology continues to advance, the quest to enhance convenience, reduce task duration, and strengthen security in daily life through such systems remains, highlighting the need for ongoing research and innovation in this field.

5.1. Theoretical Contributions

An IoT-based smart home framework for automation and intruder detection system was designed, developed, and assessed to support a comprehensive, responsive system. The proposed framework ensured the incorporation of components, such as Raspberry Pi 4, relays, PIR motion sensors, buzzers, and software, such as Google Assistant, Blynk application, Raspbian, and Node-Red. The comprehensive evaluation of command types and wireless internet connection methods contributes to the system's capabilities by encompassing Blynk button commands, Blynk voice-button commands, and Google Assistant in multiple languages. The proposed IoT-based system offers the potential for substantial advancements in convenience, efficiency, and security surveillance in daily life. In addition, this study presents a novel and inclusive assessment of the effectiveness of the proposed IoT-based system in intruder detection, employing a meticulous approach to calculate AERT and AAID. The precision of intruder detection was systematically examined using different eco-friendly wireless communication modes and varied time periods that can be

applied to assess the real-world usefulness of smart home security solutions based on IoT, particularly through accuracy and response time.

5.2. Practical Implications

Evaluating the response time of IoT-based smart home systems is critical due to its impact on system effectiveness and user experience. Home security depends on the system's ability to recognize and counteract assailants. It is critical for a residential security system to have a quick response time, as it can prevent a security violation. Robust security solutions are predicated on the ability of the system to react to any suspicious activity promptly. Responses of various system components and parameters—in response to stimuli such as PIR motion sensor latency times, communication technology, or user interaction commands—depend on system response. Additionally, response time reflects system dependability. A dependable and stable system shows a consistent and rapid response time. In contrast, response times that fluctuate or are delayed may suggest challenges in the system's design or implementation. Understanding the impact of configurations such as PIR motion-sensor delay settings on response time enables the customization of systems to meet the needs and conditions of the user. The flexibility of the IoT-based smart home framework renders the home system secure, effective, and adaptable to the requirements of users. With modifications adapted to the aims of a responsive experimental inquiry, the data were statistically evaluated with exactitude at consistent intervals.

The statistical data gathered during our study not only reveal impressive levels of accuracy and effectiveness in different wireless communication environments but also mark a significant achievement in the design and development framework of IoT-based home automation systems. The voice command recognition maintained an accuracy rate above 90%, demonstrating the system's reliability even in varying network conditions under Wi-Fi, 4G, and 5G networks. Additionally, the PIR motion sensors showed consistent effectiveness across all tested communication modes, with intruder detection accuracy remaining high. These results validate the system's robustness and adaptability to network conditions, ensuring user convenience and security in various technological circumstances. The implications of these findings are profound, potentially shaping the future of home automation systems.

5.3. Limitations and Future Work

While our comprehensive assessment of the proposed system has revealed its strengths, it has also highlighted areas where improvements can be made, sparking interest in future developments. The potential limitations discussed include IoT response time variability including voice commands, dependency only on wireless network communication modes, and the lifespan of PIR sensors. This study assessed response time variations for Google Assistant based on cloud-based translation technology, making voice commands take longer to process on wireless communication technology. This limitation concerns the system's consistency and reliability that can be improved by advancing voice command processing processes, especially for non-native English speakers who have difficulty pronouncing English fluently. The impact of different wireless communication network modes on response times was also studied, with Wi-Fi generally outperforming 4G and 5G. However, the reliance on network connectivity poses a potential vulnerability, as disruptions or network failures may compromise the system's reliability and services. Finally, PIR motion sensors have a finite operational lifespan. Continuous usage and exposure to environmental factors such as temperature variations, humidity, and other external conditions can impact the longevity and accuracy of sensors.

This roadmap for future research and development not only provides a clear direction for the field but also underscores the potential of IoT-based home automation systems. Given the findings of our study, advance design and development create numerous opportunities for enhancing IoT-based home automation systems in a sustainable way. Future research could support the real-world implementation of fail-safe mechanisms for hardware,

system operations, network communications, and renewal electrical systems to enhance system robustness. Optimizing the energy consumption of IoT devices used in the system to lead more sustainable and eco-friendly solutions, expanding the system's language capabilities, enhancing the user interface for broader accessibility, and incorporating advanced machine learning algorithms to further refine voice recognition and response times, adapting to user behaviors and preferences remain critical areas for development. Additionally, training in more algorithms can be performed using locally based multilingual systems and refining the user interface to make the system more accessible and user-friendly. User acceptance and trust, which are critical for the widespread adoption of IoT technologies in home automation, are supported by these enhancements and supplement the system's technical sturdiness.

Author Contributions: Conceptualization, P.N., M.R. and S.K.; methodology, P.N., T.U., M.R. and S.K.; software evaluation and modeling, T.U., M.R. and S.K.; validation, P.N., T.U., M.R. and S.K.; formal analysis, P.N., M.R. and S.K.; investigation, P.N., T.U., M.R. and S.K.; resources, P.N., T.U., M.R. and S.K.; data curation, P.N., T.U., M.R. and S.K.; writing—original draft preparation, P.N., T.U., M.R. and S.K.; writing—review and editing, P.N., M.R. and S.K.; visualization, P.N., T.U., M.R. and S.K.; supervision, P.N., M.R. and S.K.; project administration, P.N., T.U., M.R. and S.K.; funding acquisition, P.N., T.U. and S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. The Global Organized Crime Index. 2023. Available online: https://globalinitiative.net/analysis/ocindex-2023 (accessed on 23 December 2023).
2. Ivaschenko, O.; Nivorozhkin, A.; Nivorozhkin, E. The role of economic crisis and social spending in explaining crime in Russia: Regional panel data analysis. *East. Eur. Econ.* **2012**, *50*, 21–41. [CrossRef]
3. Lohan, V.; Singh, R.P. Home automation using internet of things. In *Advances in Data and Information Sciences*; Springer: Singapore, 2019; Volume 39, pp. 293–301. [CrossRef]
4. Samad, A.; Siddiqui, F. IoT based automation for smart sustainable homes. In Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, New Delhi, India, 27–28 February 2020. [CrossRef]
5. Netinant, P.; Vasprasert, P.; Rukhiran, M. Evaluations of effective on LWIR micro thermal camera IoT and digital thermometer for human body temperatures. In Proceedings of the 5th International Conference on E-Commerce, E-Business and E-Government, New York, NY, USA, 28–30 April 2021. [CrossRef]
6. Ahmed, S.H.; Zeebaree, S.R. A survey on security and privacy challenges in smarthome based IoT. *J. Contemp. Archit.* **2021**, *8*, 489–510.
7. Garg, R.; Gupta, S. A review on internet of thing for home automation. *Int. J. Eng. Res. Technol.* **2020**, *8*, 80–83.
8. Farooqi, A.H.; Akhtar, S.; Rahman, H.; Sadiq, T.; Abbass, W. Enhancing network intrusion detection using an ensemble voting classifier for internet of things. *Sensors* **2024**, *24*, 127. [CrossRef] [PubMed]
9. Hasan, T.; Abrar, M.A.; Saimon, M.Z.R.; Sayeduzzaman, M.; Islam, M.S. Constructing an integrated IoT-based smart home with an automated fire and smoke security alert system. *Malays. J. Sci. Adv. Technol.* **2023**, *3*, 1–10. [CrossRef]
10. Gayathri, K.S.; Thomas, T. Intrusion detection systems for internet of things. In *Handbook of Research on Intrusion Detection Systems*; IGI Global: Hershey, PA, USA, 2020; pp. 148–171. [CrossRef]
11. Majumder, A.J.; Izaguirre, J.A. A smart iot security system for smart-home using motion detection and facial recognition. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference, Madrid, Spain, 13–17 July 2020. [CrossRef]
12. Rukhiran, M.; Sutanthavibul, C.; Boonsong, S.; Netinant, P. IoT-based mushroom cultivation system with solar renewable energy integration: Assessing the sustainable impact of the yield and quality. *Sustainability* **2023**, *15*, 13968. [CrossRef]
13. Ashraf, Z.; Sohail, A.; Hameed, A.; Farhan, M.; Alotaibi, F.A.; Alnfiai, M.M. Robust and lightweight remote user authentication mechanism for next-generation IoT-based smart home. *IEEE Access* **2023**, *11*, 137899–137910. [CrossRef]
14. Liu, X.; Xu, B.; Zheng, K.; Zheng, H. Throughput maximization of wireless-powered communication network with mobile access points. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 4401–4415. [CrossRef]
15. Hellaoui, H.; Koudil, M.; Bouabdallah, A. Energy-efficient mechanisms in security of the internet of things: A survey. *Comput. Netw.* **2017**, *127*, 173–189. [CrossRef]

16. Rukhiran, M.; Wong-In, S.; Netinant, P. IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. *IEEE Access* **2023**, *11*, 22767–22787. [CrossRef]
17. Viswanath, S.K.; Yuen, C.; Tushar, W.; Li, W.-T.; Wen, C.-K.; Hu, K.; Chen, C.; Liu, X. System design of the internet of things for residential smart grid. *IEEE Wirel. Commun.* **2016**, *23*, 90–98. [CrossRef]
18. Al Faruque, M.A.; Vatanparvar, K. Energy management-as-a-service over fog computing platform. *IEEE Internet Things J.* **2016**, *3*, 161–169. [CrossRef]
19. Khudhair Al-Gburi, M.; Ali Abdul-Rahaim, L. Secure smart home automation and monitoring system using internet of things. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *28*, 269. [CrossRef]
20. Netinant, P.; Amatyakul, A.; Rukhiran, M. Alert intruder detection system using passive infrared motion detector based on internet of things. In Proceedings of the 2022 5th International Conference on Software Engineering and Information Management, New York, NY, USA, 21–23 January 2022. [CrossRef]
21. Tao, M.; Zuo, J.; Liu, Z.; Castiglione, A.; Palmieri, F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Gener. Comput. Syst.* **2018**, *78*, 1040–1051. [CrossRef]
22. Beuran, R.; Wang, J.; Zhao, M.; Tan, Y. IoT security training for system developers: Methodology and tools. *Internet Things* **2023**, *24*, 100931. [CrossRef]
23. Yang, J.; Sun, L. A comprehensive survey of security issues of smart home system: "Spear" and "Shields", theory and practice. *IEEE Access* **2022**, *10*, 124167–124192. [CrossRef]
24. Allifah, N.M.; Zualkernan, I.A. Ranking security of IoT-based smart home consumer devices. *IEEE Access* **2022**, *10*, 18352–18369. [CrossRef]
25. Likhitha, K.; Malineni, S.; Jampani, N.; Prasanna, N.L. Home security system using PIR sensor-IoT. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2019**, *5*, 497–500. [CrossRef]
26. Chen, X.-Y.; Wen, C.-Y.; Sethares, W.A. Multi-target PIR indoor localization and tracking system with artificial intelligence. *Sensors* **2022**, *22*, 9450. [CrossRef] [PubMed]
27. Palaniapan, S.; Kollathodi, M.A. Real time implementation of embedded devices as a security system in intelligent vehicles connected via Vanets. *Int. J. Electr. Comput. Eng.* **2019**, *9*, 4788–4797. [CrossRef]
28. Roslina, R.; Amelia, A.; Pranoto, H.; Sundawa, B.V. System of smart detection and control to electrical energy for saving of electrical energy consumption. *Bull. Electr. Eng. Inform.* **2021**, *10*, 2454–2465. [CrossRef]
29. Netinant, P.; Rukhiran, M.; Rattanakorn, P. Development of smart light control and intruder detection with voice and motion based on internet of things using Raspberry Pi. In Proceedings of the 6th International Conference on Business and Information Management, Guangzhou, China, 26–28 August 2022. [CrossRef]
30. Panigrahi, S.K.; Goswami, V.; Apat, H.K.; Barik, R.K.; Vidyarthi, A.; Gupta, P.; Alharbi, M. An interconnected IoT-inspired network architecture for data visualization in remote sensing domain. *Alex. Eng. J.* **2023**, *81*, 17–28. [CrossRef]
31. Kanellopoulos, D.; Sharma, V.K.; Panagiotakopoulos, T.; Kameas, A. Networking architectures and protocols for IoT applications in smart cities: Recent developments and perspectives. *Electronics* **2023**, *12*, 2490. [CrossRef]
32. Satapathy, L.M.; Bastia, S.K.; Mohanty, N. Arduino based home automation using internet of things (IoT). *Int. J. Pure Appl. Math.* **2018**, *118*, 769–778.
33. Sharif, H.; Despot, I.; Uyaver, S. A proof of concept for home automation system with implementation of the internet of things standards. *Period. Eng. Nat. Sci.* **2018**, *6*, 95–106. [CrossRef]
34. Stolojescu-Crisan, C.; Crisan, C.; Butunoi, B.-P. An IoT-based smart home automation system. *Sensors* **2021**, *21*, 3784. [CrossRef] [PubMed]
35. Irugalbandara, C.; Naseem, A.S.; Perera, S.; Kiruthikan, S.; Logeeshan, V. A secure and smart home automation system with speech recognition and power measurement capabilities. *Sensors* **2023**, *23*, 5784. [CrossRef]
36. Venkatraman, S.; Overmars, A.; Thong, M. Smart home automation—Use cases of a secure and integrated voice-control system. *Systems* **2021**, *9*, 77. [CrossRef]
37. Iliev, Y.; Ilieva, G. A framework for smart home system with voice control using NLP methods. *Electronics* **2022**, *12*, 116. [CrossRef]
38. Dbritto, V.; Carwalo, T.; Chaudhari, P.; Solaskar, S.; Machado, S. Smart home automation system. In Proceedings of the International Conference on Recent Advances in Computational Techniques, Maharashtra, India, 26–27 June 2020. [CrossRef]
39. Zaro, F.; Tamimi, A.; Barakat, A. Smart home automation system. *Int. J. Eng. Innov. Res.* **2021**, *3*, 66–88. [CrossRef]
40. Shehab, M.J.; Kassem, I.; Kutty, A.A.; Kucukvar, M.; Onat, N.; Khattab, T. 5G Networks towards smart and sustainable cities: A review of recent developments, applications and future perspectives. *IEEE Access* **2022**, *10*, 2987–3006. [CrossRef]
41. Huseien, G.F.; Shah, K.W. A review on 5G technology for smart energy management and smart buildings in Singapore. *Energy AI* **2022**, *7*, 100116. [CrossRef]
42. Mazhar, T.; Malik, M.A.; Haq, I.; Rozeela, I.; Ullah, I.; Khan, M.A.; Adhikari, D.; Ben Othman, M.T.; Hamam, H. The Role of ML, AI and 5G technology in smart energy and smart building management. *Electronics* **2022**, *11*, 3960. [CrossRef]
43. Gohar, A.; Nencioni, G. The Role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability* **2021**, *13*, 5188. [CrossRef]
44. Afreen, H.; Kashif, M.; Shaheen, Q.; Alfaifi, Y.H.; Ayaz, M. IoT-based smart surveillance system for high-security areas. *Appl. Sci.* **2023**, *13*, 8936. [CrossRef]

45. Al-Jazzar, S.O.; Aldalahmeh, S.A.; McLernon, D.; Zaidi, S.A.R. Intruder localization and tracking using two pyroelectric infrared sensors. *IEEE Sens. J.* **2020**, *20*, 6075–6082. [CrossRef]
46. Fang, L.; Wu, Y.; Wu, C.; Yu, Y. A nonintrusive elderly home monitoring system. *IEEE Internet Things J.* **2021**, *8*, 2603–2614. [CrossRef]
47. Erden, F.; Velipasalar, S.; Alkar, A.Z.; Cetin, A.E. Sensors in assisted living: A survey of signal and image processing methods. *IEEE Signal Process. Mag.* **2016**, *33*, 36–44. [CrossRef]
48. Wang, P.; Lu, X.; Sun, H.; Lv, W. Application of speech recognition technology in IoT smart home. In Proceedings of the 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference, Chongqing, China, 11–13 October 2019. [CrossRef]
49. Abidi, E.; Asnawi, A.L.; Azmin, N.F.M.; Jusoh, A.Z.; Ibrahim, S.N.; Ramli, H.A.M.; Malek, N.A. Development of voice control and home security for smart home automation. In Proceedings of the 2018 7th International Conference on Computer and Communication Engineering, Chongqing, China, 11–13 October 2019. [CrossRef]
50. Chenxuan, H. Research on speech recognition technology for smart home. In Proceedings of the 2021 IEEE 4th International Conference on Automation, Electronics and Electrical Engineering, Shenyang, China, 19–21 November 2021. [CrossRef]
51. Gunawan, T.S.; Mokhtar, M.N.; Kartiwi, M.; Ismail, N.; Effendi, M.R.; Qodim, H. Development of voice-based smart home security system using Google voice kit. In Proceedings of the 2020 6th International Conference on Wireless and Telematics, Yogyakarta, Indonesia, 3–4 September 2020. [CrossRef]
52. Wang, H.H. Speech recorder and translator using Google cloud speech-to-text and translation. *J. IT Asia* **2021**, *9*, 11–28. [CrossRef]
53. Martín, B.S. Translation Quality Assessment of Google Translate and Microsoft Bing Translator. Available online: http://uvadoc.uva.es/bitstream/handle/10324/22596/TFG_F_2017_7.pdf?sequence=1&isAllowed=y (accessed on 24 December 2023).
54. Lee, H.-T.; Chen, R.-C.; Chung, W.-H. Combining voice and image recognition for smart home security system. In *Lecture Notes in Electrical Engineering*; Springer: Singapore, 2019; pp. 212–221. [CrossRef]
55. Ali, A.-E.A.; Mashhour, M.; Salama, A.S.; Shoitan, R.; Shaban, H. Development of an intelligent personal assistant system based on IoT for people with disabilities. *Sustainability* **2023**, *15*, 5166. [CrossRef]
56. Daengsi, T.; Yochanang, K.; Wuttidittachotti, P. A Study of perceptual VoIP quality evaluation with Thai users and codec selection using voice quality—Bandwidth tradeoff analysis. In Proceedings of the 2013 International Conference on ICT Convergence, Jeju, Republic of Korea, 14–16 October 2013. [CrossRef]
57. Wutiwiwatchai, C.; Hansakunbuntheung, C.; Rugchatjaroen, A.; Saychum, S.; Kasuriya, S.; Chootrakool, P. Thai text-to-speech synthesis: A review. *J. Intell. Inform. Smart Technol.* **2017**, *2*, 1–8.
58. Rukhiran, M.; Buaroong, S.; Netinant, P. Software development for educational information services using multilayering semantics adaptation. *Int. J. Serv. Sci. Manag. Eng. Technol.* **2022**, *13*, 1–27. [CrossRef]