

Article

Smart Home Automation—Use Cases of a Secure and Integrated Voice-Control System

Sitalakshmi Venkatraman ^{*}, Anthony Overmars  and Minh Thong

Department of Business and Construction, Melbourne Polytechnic, Preston, VIC 3072, Australia;
AnthonyOvermars@melbournepolytechnic.edu.au (A.O.); minhthong561@gmail.com (M.T.)

* Correspondence: SitaVenkat@melbournepolytechnic.edu.au

Abstract: Smart home automation is expected to improve living standards with the evolution of internet of things (IoT) that facilitate the remote control of residential appliances. There are, however, several factors that require attention for broader successful consumer adoption. This paper focusses on three key barriers: (i) different underlying technologies requiring an integrated voice-based control for ease of use, (ii) lack of trust due to security and privacy concerns, and (iii) unawareness of the use of machine intelligence by users for exploiting the full potential of smartness. Voice-controlled home environments are possible with cloud-based solutions that are being deployed commercially. However, there are drawbacks due to non-standard voice channels and commands with delays in meeting the required response time for real-time services. Adoption is also required to meet with the expected goals of simplicity, security, and integration. To address these barriers, we propose a model integrating IoT services and wireless technologies for developing a secure smart home automation with a voice-controlled artificial intelligence system. We demonstrate the model's application in a variety of practical use cases, by implementing a secure and smart voice-based system for an integrated control of several home devices seamlessly.

Keywords: smart home automation; internet of things (IoT); voice-controlled systems; security and privacy; integrated solution



Citation: Venkatraman, S.;

Overmars, A.; Thong, M. Smart

Home Automation—Use Cases of a Secure and Integrated Voice-Control System. *Systems* **2021**, *9*, 77. <https://doi.org/10.3390/systems9040077>

Received: 26 August 2021

Accepted: 26 October 2021

Published: 28 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The momentous evolution of Internet of Things (IoT) has enabled the realisation of smart homes of the future [1]. Ideally, IoT devices in a smart home environment can communicate seamlessly with one another via the internet, with intelligent capabilities for big data-based decision making [2,3]. While there is an expected improvement in the quality of human life, the current gaps in practical implementation form barriers in the adoption of smart devices in home environments [4,5].

Studies show that the potential value of smart homes can be realised if existing barriers such as interoperability among IoT systems, security and privacy concerns, and usability of IoT data gaps are addressed [6,7]. Further, there is lack of awareness for fully exploiting the capabilities of different IoT devices to use machine intelligence for a voice-based integrated smart home automation [8,9]. Currently, users consider health and fitness as the two main categories of applications for successful IoT adoption and a range of devices and appliances are still emerging towards establishing smart homes of the future [10,11]. Greater economic considerations are given to human productivity in the office environment as well as safety in factories or worksites for workplace automation. Hence, research and commercial development have focused on business-to-business applications rather than consumer applications [12]. However, some of the smartness with interconnected thermostat devices, self-guided vacuum cleaners, automated lighting, door entry/security systems, kitchen and laundry appliances could be employed to achieve chore automation, energy efficiency and other areas of economic value in a home environment [13]. It is important to have a

customer focus in providing any smart service in home automation systems to enhance user adoption [14]. This forms the main motivation for this paper. Our aim is to propose a secure and integrated smart home automation model using a voice-based command and control. Further, to enable the perceived value for consumers, it is important to implement any proposed model, with typical use cases. We consider this approach for demonstrating how an easy-to-use voice-based smart home environment could be achieved.

In recent years, users prefer to interact with digital devices using voice as an effective and natural mode of communication [3,9]. Voice technologies have emerged to employ machine intelligence for a smart control of home appliances offering hands-free and eye-free operations along with using the IoT pervasive environments more effectively [15,16]. However, commercially available voice-assisted technologies lack personalisation, standardisation, security, and integration as they focus on only specific applications. Such off-the-shelf solutions are not capable of providing a common platform for all types of users, including the elderly, to interact with several disparate IoT devices in a home environment [17–19]. Recent studies discuss design implications and the requirement of voice-assisted features tailored to meet the needs of visually impaired people as well as older adults for a better adoption of smart home technologies [20,21]. Further, smart homes of today exhibit gaps in privacy norms with the deployment of several third-party smart services that can encroach beyond the boundaries of home, leading to security and privacy threats [22].

In this paper, we take a modest step to fill the gap in the literature with the aim to achieve a smart home automation system with essential features sustainable for the future. We propose a secure and integrated model, connecting IoT devices and appliances, to implement a smart home automation with a voice-based command and control approach. Our system leverages the seamless connectivity of IoT platforms to automatically identify devices over a securely deployed network. The main consideration in proposing the system model is to allow users to operate remotely, via their voice, with addressing the concerns related to usability, trust, and the overheads of managing several IoT devices in a typical home environment. Furthermore, by implementing a prototype of the system with a variety of use cases, our aim is to demonstrate the simplicity and viability of our proposed model for any smart home environment.

Overall, the key contributions of our work are as follows:

(i) Proposal of a unique model that combines low-cost, scalable, and simple to configure end-to-end security of IoT along with voice-controlled command operations of various devices in a smart home.

(ii) Application of a customised virtual private network (VPN) using the Raspberry Pi development platform with sensors, as a single embedded system to connect securely with personalised user authentication, granting access to authorised devices within a IoT network of a smart home.

(iii) Development of a voice-control system to recognise speech commands, using the smartphone of an authenticated user, to operate smart devices intelligently and securely via the customised VPN that connects the Raspberry Pi platform to IoT devices in a smart home.

(iv) Demonstration of our proposed model's implementation and practical viability with devices such as a lighting system, music player, computer, and water tank, upon which to execute different speech commands to switch on/off certain sensors, to play a particular song, to perform a voice-based online search or to even monitor and control the water flow from a water tank remotely in a home environment.

The rest of the paper is organized as follows: Section 2 provides the background, highlighting previous research and contributions of this work. In Section 3, we describe our proposed model for a secure home automation system that is voice-enabled. In Section 4, we demonstrate the use cases of our proposed system and their implementation. Finally, we provide concluding remarks and future research directions in Section 5.

2. Background and Previous Work

In the past couple of decades, wireless communication technologies have evolved rapidly [23–26]. In the late 2000s, we implemented a remote-controlled irrigation system which established wireless communication among three different farms (vineyard, apple orchard and flood irrigated pasture) located at widely dispersed locations in the Goulbourn Valley of Australia [27]. During that time, 3G wireless technology was developed and our remote-controlled irrigation system was deployed in a new 3G network infrastructure. Real-time communication and remote access on such a large-scale deployment was achieved using remote desktop sessions through port 3389. Subsequently, as technologies evolve, we witness security breaches and vulnerabilities, and this type of remote access and control is no longer considered secure. In a more recent work, we deployed a remote-controlled water tank system, which allowed access to IoT devices via the smart phone with secure communication to the sensors of several water tanks as a large-scale deployment through a virtual private network (VPN) [28]. Sustainable development and successful user acceptance of such smart technologies depend much on the ease-of-use, operational integration, and establishment of trust, apart from economy and robustness. Hence, this paper considers the next level of our research advancement in developing an integrated voice-control system that offers a secure and personalised service to consumers. We take an initial step in this direction with the development of a smart home automation system in this paper.

A literature review of recent studies indicates that voice technology combined with the latest wireless technologies capable of seamless connectivity of IoT devices is trending towards successful consumer adoption [9,10,14,29]. The most popular context of its application is in Smart Home Automation, to serve as a personalised assistant [30]. Recently, a voice control system for smart home implemented with cloud data storage was studied [31]. The system was based upon Alexa Voice Service connected to Amazon Echo in a cloud environment. It has come to light that Alexa is “always on” and records all voice activity in the home even when it is not intended to be activated. Such data collection may raise privacy concerns, even though this is in line with the terms of use agreement that users click and agree to. In addition, breaches of these voice data have occurred. Over a period of time, technological advancements have opened up many ways of how this endless stream of personal voice information can be accessed and used, not in a way that users had intended, and the possibility of misuse has started to raise trust concerns [32,33]. Further, recent capabilities of artificial intelligence (AI) to interpret large swaths of an individual’s voice along with big data technologies have led to real concerns as to how this information might be used [34]. One impact could be to push direct targeted marketing campaigns for influencing an individual’s purchasing choices. AI-induced voice recognition has enabled many banking and government organisations to switch to online voice identification. Voice profiling and the storage of this biometric data with an individual’s profile can even lead to identity theft. Overall, we find that the “always on” voice data collection in such cloud-based systems has drawn the spectre of public opinion and concerns [5,15,35].

The solution to the above-mentioned concerns is to leverage the positive aspects of voice-based AI engines that have become very efficient in terms of software development and can now be run by local processing elements rather than in the cloud data centres. Since home automation systems require only small-scale deployments unlike commercial industry automation systems, voice command datasets are relatively small and can even be run by devices such as Raspberry Pi [7]. This is advantageous as it brings the control back to the individual user and mitigates the leakage of personal voice information. Hence, this research project aims to develop a voice-controlled AI application to run on a Raspberry Pi to control various IoT devices over the internet using a mobile phone in a secure home environment, including the water tank in a remote backyard location. This paper brings together several key elements from earlier work [27,28]. In this research study, we advance further to securely integrate various IoT devices wirelessly at home along with the enhanced features of a light-weight voice-assisted AI system. Thereby, we develop the initial steps

to pave way for a sustainable and acceptable home automation towards enabling remote command and control capabilities at the local home computing level without the need for large-scale AI capabilities from a cloud environment.

3. Proposed Model for a Secure Smart Home Automation System

In recent years, technological innovations have provided tremendous growth in IoT. This combined with advances in ubiquitous computing are converging technologies for smart homes of the future [1,3]. However, security and privacy (and trust), form the key barriers in the expected adoption. While research shows several ways of implementing security in the IoT context, the main concerns are lack of simplicity, adaptability, integration, and low-cost deployment in a smart home environment. We propose a secure and integrated smart home automation system as a modest initial step to address these existing limitations. The proposed model aims to:

- (i) Combine low-cost, scalable, simple to configure end-to-end security;
- (ii) Apply a customised virtual private network;
- (iii) Employ a voice-controlled AI system to recognise speech commands;
- (iv) Demonstrate the practical viability through an easy-to-use implementation with typical use cases in a smart home environment.

For every device in a smart home, the proposed model is aimed at providing an integrated voice control system with a secure connection to the IoT network. This is achieved by establishing end-to-end security using uniquely customized VPN technology. A practically viable deployment is implemented with smartphone-based speech recognition, for command and control of the devices. More importantly, we aim to demonstrate the practical application of the model by implementing a smart home automation system in a typical home environment with selected appliances and IoT devices to securely connect and operate with voice-assisted commands.

The proposed smart home automation system ensures the security and privacy of each user by connecting and configuring the IoT devices using OpenVPN and with a smartphone to control the devices, enhancing our previous work [28]. Users will be able to interact with the system with non-native English using a machine intelligent software platform. This is programmed in Python language with API commands to communicate with simple mobile phones that do not require a sophisticated voice system. We employ opensource libraries to develop the required voice recognition component of the system. This is used to detect different speech sounds and voice-based commands to operate various IoT devices to realize the unique advantage of having both convenience and security. Low-cost embedded controllers process each command and then send it to the appropriate device within the smart home environment through its relay controller. We make use of the Raspberry Pi platform as it provides several options to connect IoT devices, home appliances and sensors in a simple and efficient way. A pictorial representation of the proposed model is shown in Figure 1. This shows how a customized VPN is deployed to securely connect a mobile phone to the Raspberry Pi wirelessly to send the user's speech commands. The proposed integrated voice-recognition system executes user commands to operate, monitor and control various devices in a smart home.

As shown in Figure 1, the proposed smart home architecture consists of three main components: (i) a secure VPN customized to connect smart devices to the Raspberry Pi, establishing end-to-end security as one embedded unit in a smart home; (ii) an integrated Smart Home connecting the Raspberry Pi breadboard directly through a relay driver to control the sensors and devices such as a lighting system, music player, water tank, air-conditioning unit, computer and other external smart systems via the internet; (iii) a Mobile Interface with a voice-based recognition module for authorized users to give speech commands through their smartphone's microphone to communicate securely to the Smart Home devices. These components work together via the secure IoT network established using the Raspberry Pi platform to cater to the user-based command and control system.

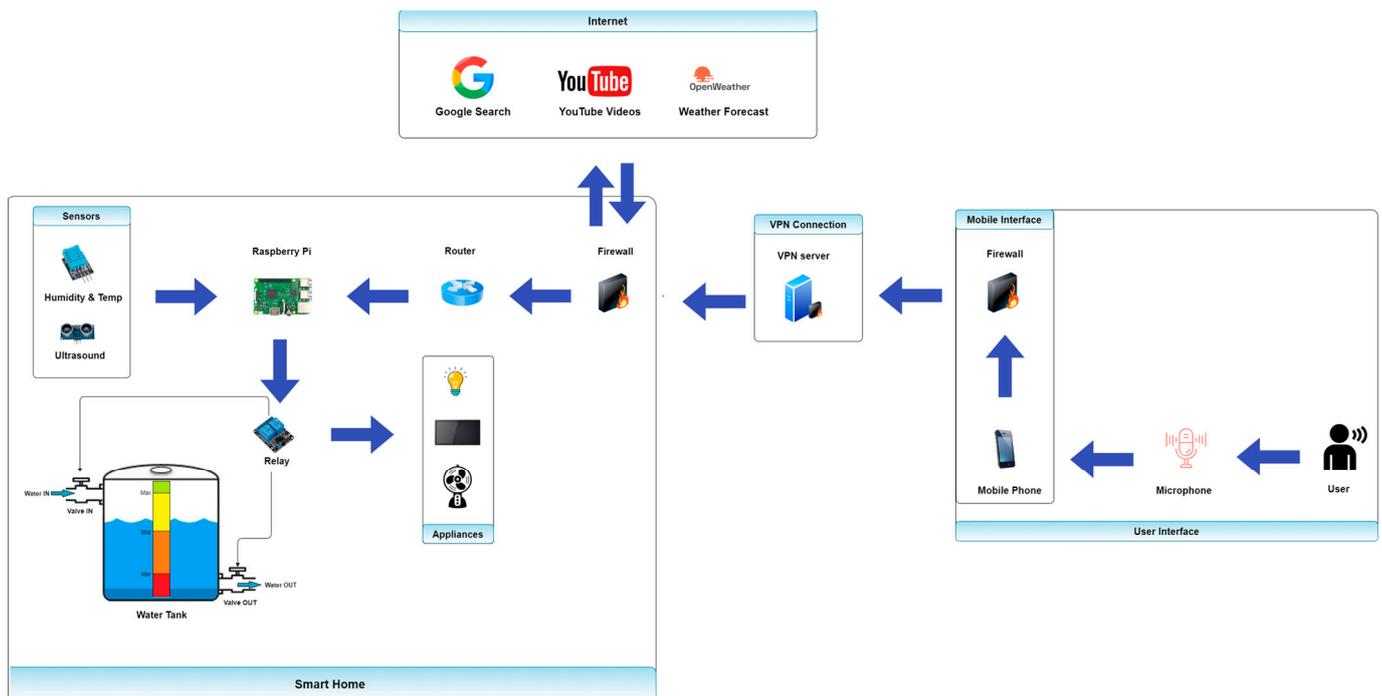


Figure 1. Proposed smart home automation.

4. Implementation of a Secure Smart Home Automation System

We demonstrate the application of the proposed system to a unique context of a scalable IoT infrastructure within a smart home environment. Privacy and security are the main barriers for a practical implementation of home automation systems and several studies have identified the key requirement of IoT security [36,37]. With the background of a comprehensive study on the vulnerabilities and security attacks of an IoT network, we advance further in this research work to address these [38–40]. Firstly, we implement an end-to-end security model that we had developed previously [28], enhancing it to use a uniquely customized VPN technology for the smart home use case in this work. We address the high overheads and complex configurations of OpenVPN by employing smart mobile apps that readily support VPN client interfaces to access the smart home devices instantly in a securely authenticated manner, as shown in Figure 2; we demonstrate the securely established connection to the IoT devices, with the water tank use case as an illustration in the home environment.

In the next step, the Raspberry Pi controller is connected via the secure VPN to the display device and the IoT devices such as temperature sensors, lighting systems, music players, mobile phones, water tank, and other smart home appliances. Figure 3 shows the actual deployment of the Raspberry Pi breadboard and selected sensors and IoT devices. As shown in Figure 3, we integrate a relay channel, humidity and temperature sensor, distance sensor and voice input sensor with the Raspberry Pi breadboard. It illustrates the connections of our system to the IoT server to facilitate control of these devices via VPN wireless technologies.

In this work, the required programming codes to serve as a mobile app for controlling the sensors that were connected to Raspberry Pi. Figure 4 shows the deployment of a water tank's sensors and valves connected to the Raspberry Pi via a breadboard in the initial prototype testing phase. We tested the codes using an opensource software tool called NodeRed using NodeJS and JavaScript code. Using the mobile application, we could control the flow of water in and out of the tank. Once the water tank was successfully deployed and tested within our secure home smart automation system, we used the breadboard to extend the number of ports on the Raspberry Pi to connect other

devices of the smart home. We customized the codes for each sensor and employed voice-based commands developed in Python to operate various devices in the smart home. The AI engine for voice recognition was then trained to learn various home user voices to personalize the home automation system.

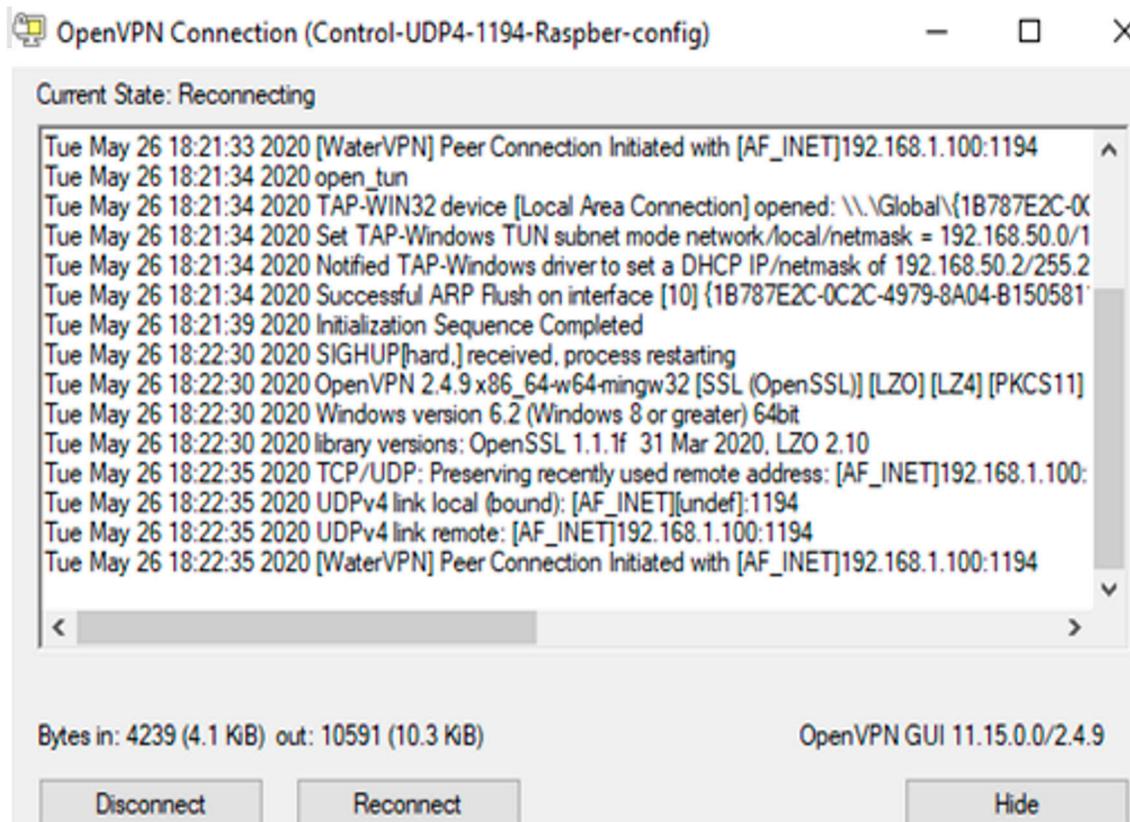


Figure 2. VPN-based authentication for remote smart home access.

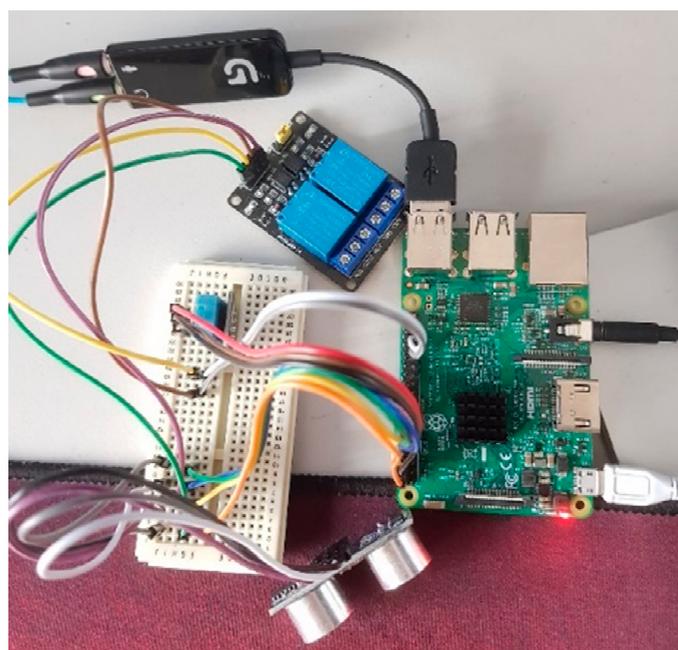


Figure 3. Integrated device controls with raspberry Pi breadboard.



Figure 4. Initial deployment of secure smart water tank automation system.

In the final evaluation phase, the voice recognition module (robot) of the AI engine was implemented using a machine learning approach. This was tested to identify the user voice as well as undergo supervised training iterations after each evaluation, to enhance its robustness. We tested different scenarios by sending speech commands to perform specific actions to control various devices in the smart home. The speech recognition robot was initially trained using music searches in a browser. This was then extended using a pre-defined set of keywords such as on, off, open, close, date, water level, and others relating to weather parameters as well. Figure 5 demonstrates the output of the training underwent by the robot to display the current date when voice-based command was used. For the voice-based command given by the user such as “What is the date today?”, the robot recognizes the command. The robot interprets the command and the current date is displayed as the result. These tests performed show that the speech was correctly translated to text in English. After the learning process, the robot could obtain the stored data from the computer connected in the secure IoT network in the smart home for the correct voice recognition of different users. Figure 5 also shows the results of speech recognition training, including user-friendly spare time conversation of the robot by saying “I’m Listening” to invite the user to make further commands.

We implemented the use case of searching the web browser for various needs of the home user. For instance, Figure 6 shows how a voice-based command is used to search in the Web browser to play any music based on the user’s requirement. The robot is also intelligent to respond suitably with user errors. For instance, if some music is already in play mode when the user prompts to play any music, the robot will respond to the user that the music is playing, as illustrated in Figure 6. Another application of the robot that is useful for people with visual impairment or any disability is using voice to browse the Web for shopping. Figure 7 shows the result of voice-based search for an auto-recognised user to seek some information about furniture from the Web. The page located on the Web could be even printed or saved in the mobile phone as required by the user.

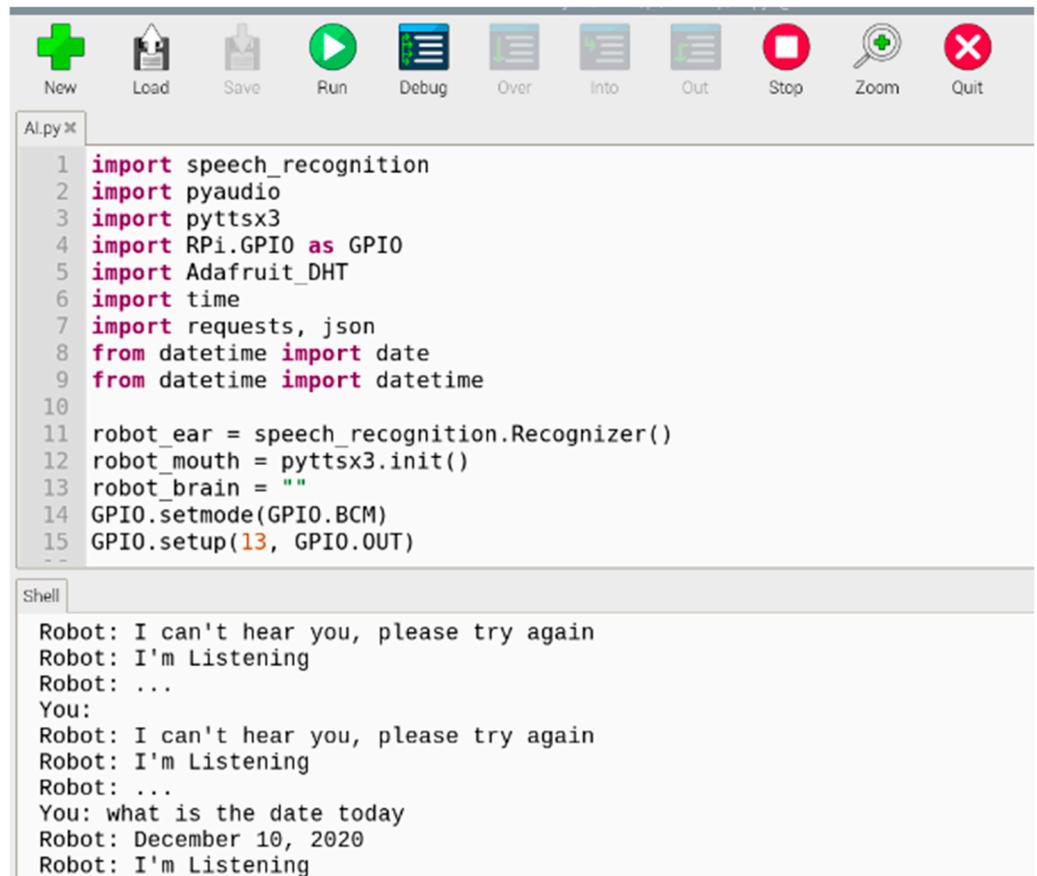


Figure 5. Speech recognition training results.

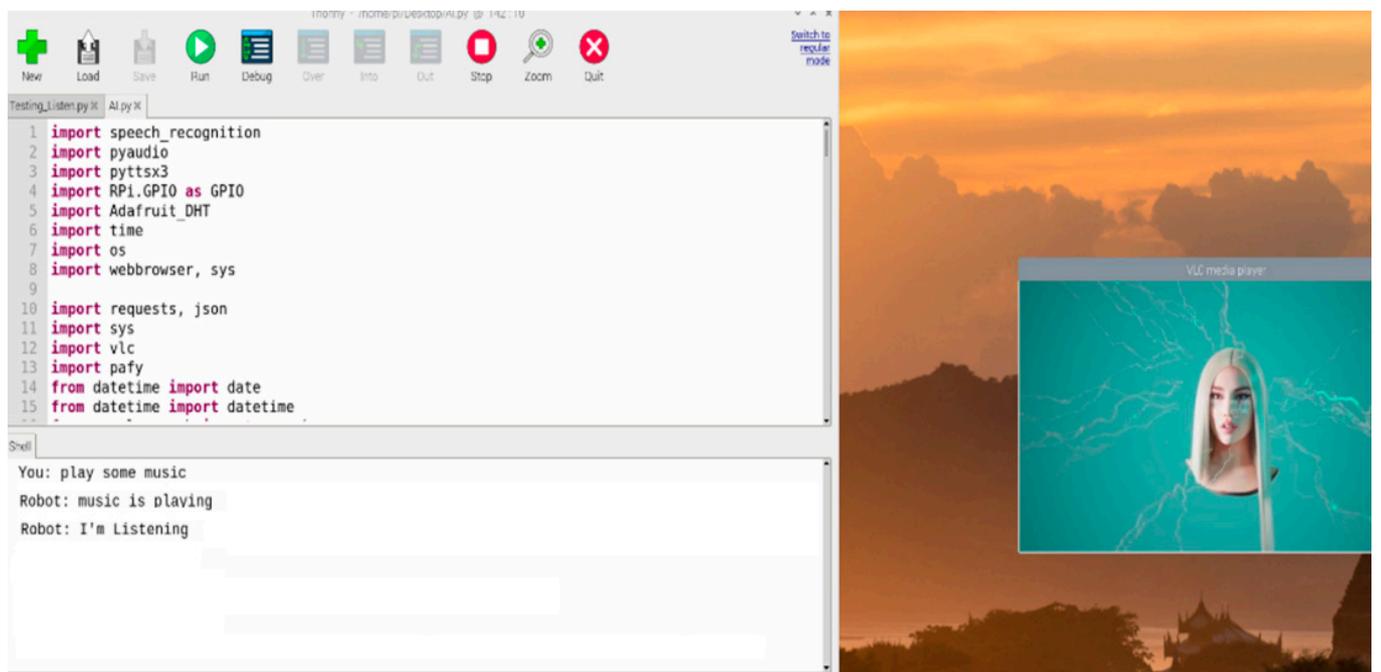


Figure 6. Voice-based testing to play music via the web.

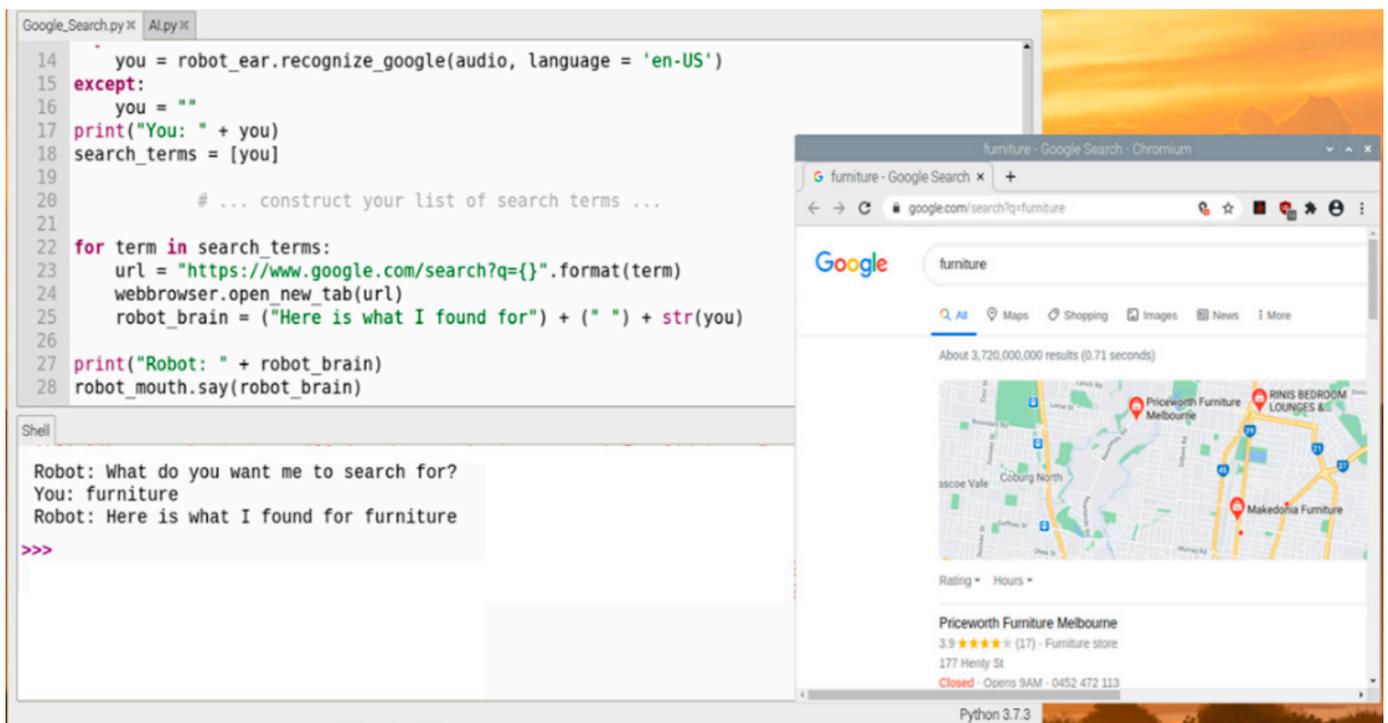
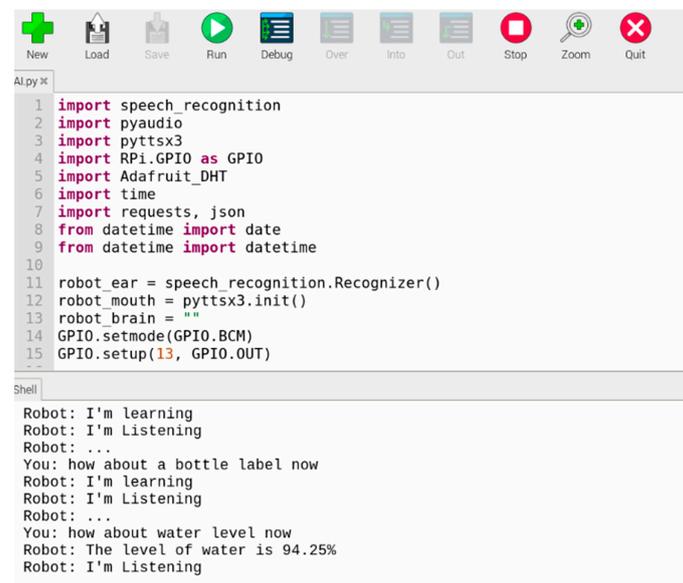


Figure 7. Voice-based testing for user's search for information from the web.

We established the robustness of the voice-based control of the smart home automation system by training the robot to recognize and differentiate homophones or words that sound similar. We tested this with homophones related to the water tank device operations to perform the correct actions. For instance, we tested the system by asking an incorrect question "What is the bottle label?", which sounds similar to the desired question "What is the water level?". The robot demonstrated that it could learn well to identify homophones present in a user command that were incorrectly used. When the correct question was asked, the system activated the data from the right sensor in the water tank to output the water level. For the water tank use case, we have installed a sensor for detecting the water level and two smart sensor valves, one for water inlet (Valve 1) and the other for water outlet (Valve 2). The program code was written in Python language for setting various rules and to calculate the percentage of water level from the water tank sensor. For instance, the speech recognition robot was connected to the water sensor to output the data as the calculated percentage of water. Figure 8 demonstrates the results of the tests performed to establish the robustness of the system via a mobile app. It shows that the speech recognition robot could output the correct result of 67% as the level of water in the tank.

Further, we explored alternative ease-of-use approaches in addition to voice recognition AI by employing smartphone controls effectively. To enhance the usability of the smart home automation, we deployed the user interface in a mobile app. This would cater to end-users who would prefer to monitor the water level and operate the water tank remotely in the home environment system using the mobile app. Figure 9 demonstrates a dashboard display to illustrate how the status of the second valve outlet (Valve 2) sensor of the smart water tank is automatically set to "on" and is shown by Water Out toggle and the current water level in real-time. The display continuously shows the water level reducing as the water is let out remotely from the water tank. By having this control setting, the smart home automation system allows the user to open the water tank valve remotely using the smartphone's app. This feature will allow water to be used for situations such as watering plants in the garden when the user is in a remote location. The configuration for the controls could be customised by the user such that "if the water level is greater than 15% of tank capacity, turn ON the valve". In addition, using Python libraries, the

smart home automation system is able to gather external weather parameters outside the home environment such as atmospheric pressure, humidity and temperature. Integrating these with the water tank controls would lead to more intelligent control settings and automatic actions.



```
Al.py x
1 import speech_recognition
2 import pyaudio
3 import pyttsx3
4 import RPi.GPIO as GPIO
5 import Adafruit_DHT
6 import time
7 import requests, json
8 from datetime import date
9 from datetime import datetime
10
11 robot_ear = speech_recognition.Recognizer()
12 robot_mouth = pyttsx3.init()
13 robot_brain = ""
14 GPIO.setmode(GPIO.BCM)
15 GPIO.setup(13, GPIO.OUT)
--
Shell
Robot: I'm learning
Robot: I'm Listening
Robot: ...
You: how about a bottle label now
Robot: I'm learning
Robot: I'm Listening
Robot: ...
You: how about water level now
Robot: The level of water is 94.25%
Robot: I'm Listening
```

Figure 8. Robustness of speech recognition for smart water tank control.

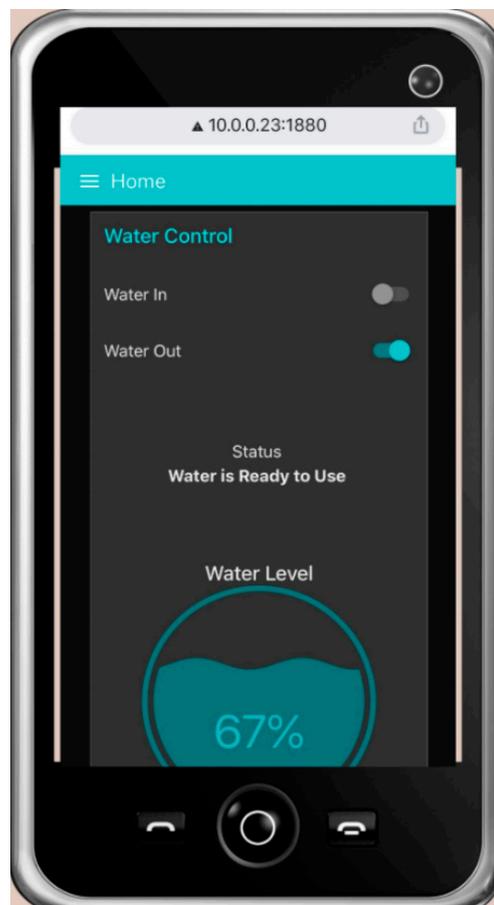


Figure 9. Smart phone interface for smart water tank control.

Overall, the proposed smart home automation system is developed to securely adapt for deploying different IoT use case scenarios in a home environment as demonstrated in this work and to support our future ongoing research in this direction. The proposed framework is sustainable, catering to different user interfaces and communication preferences, as a home user's requirements could change over time and with the evolution of new wireless technologies and IoT devices in smart homes. Future research considerations could also include the use of suitable energy management schemes to embrace the green energy agenda and to address socioeconomic challenges in improving the consumer service satisfaction of smart homes for successful adoption [41,42].

5. Conclusions and Future Research

This paper proposed the convergence of IoT in a secure infrastructure model, distributed across multiple platforms, in remote locations with AI voice control. We demonstrated an integrated implementation of the model for smart home automation system by considering several challenges, principally:

- (i) The requirement of different underlying technologies to integrate voice-based control for ease-of-use;
- (ii) Lack of trust and usability due to security/privacy concerns and affordability;
- (iii) Unawareness of the application of machine intelligence by users for exploiting the full potential of smartness to control IoT devices in a home environment.

This original research work resulted in three key contributions. Firstly, we developed a voice-recognition AI engine as a personal assistant robot to successfully become trained with user voice and to remotely control various IoT sensors and devices using a smartphone. Secondly, the proposed unique model provided a low-cost, scalable, and simple to configure end-to-end security of IoT devices addressing privacy threats that could be associated with any third-party services. Thirdly, several use cases in a typical home environment were illustrated to demonstrate the practical viability and deployment of a secure and easy-to-use system, paving the way for a sustainable smart home consumer adoption.

Future work would explore several other use cases to arrive at a more comprehensive suite of integrated IoT devices in a smart home. The voice AI engine will also undergo deep learning approaches for its training. Further, user experiences with the system to enhance the user interface and service satisfaction will be explored.

Author Contributions: Conceptualization, S.V.; methodology, S.V. and A.O.; resources, S.V., A.O. and M.T.; software, M.T.; validation, S.V., A.O. and M.T.; writing—original draft preparation, S.V.; writing—review and editing, S.V. and A.O.; and supervision, S.V. and A.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Helal, S.; Bull, C. From Smart Homes to Smart-Ready Homes and Communities. *Dement. Geriatr. Cogn. Disord.* **2019**, *47*, 157–163. [[CrossRef](#)]
2. Stojkoska, B.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [[CrossRef](#)]
3. Moeid, I.; Hana, S.; Amer, Z. Next Generation Home Automation System Based on Voice Recognition. In Proceedings of the 6th International Conference on Engineering & MIS 2020, Almaty, Kazakhstan, 14–16 September 2020.
4. Hui, T.K.; Sherratt, R.S.; Sánchez, D.D. Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Futur. Gener. Comput. Syst.* **2017**, *76*, 358–369. [[CrossRef](#)]

5. Guhr, N.; Werth, O.; Blacha, P.P.H.; Breitner, M.H. Privacy concerns in the smart home context. *SN Appl. Sci.* **2020**, *2*, 247. [[CrossRef](#)]
6. Lawal, K.; Rafsanjani, H.N. Trends, benefits, risks, and challenges of IoT implementation in residential and commercial buildings. *Energy Built Environ.* **2021**. [[CrossRef](#)]
7. Li, R.Y.M.; Li, H.C.Y.; Mak, C.K.; Tang, T.B. Sustainable Smart Home and Home Automation: Big Data Analytics Approach. *Int. J. Smart Home* **2016**, *10*, 177–198. [[CrossRef](#)]
8. Chankdak, N.; Joshi, A. An Intelligent Remote Controlled System for Smart Home Automation. *Int. Res. J. Eng. Technol.* **2018**, *5*, 890–892.
9. Singh, P.; Nayak, P.; Datta, A.; Sani, D.; Raghav, G.; Tejpal, R. Voice Control Device using Raspberry Pi. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; pp. 723–728.
10. Ismail, A.; Abdlerazek, S.; El-Henawy, I.M. Development of Smart Healthcare System Based on Speech Recognition Using Support Vector Machine and Dynamic Time Warping. *Sustainability* **2020**, *12*, 2403. [[CrossRef](#)]
11. Perez-Pozuelo, I.; Zhai, B.; Palotti, J.; Mall, R.; Aupetit, M.; Garcia-Gomez, J.M.; Taheri, S.; Guan, Y.; Fernandez-Luque, L. The future of sleep health: A data-driven revolution in sleep science and medicine. *NPJ Digit. Med.* **2020**, *3*, 42. [[CrossRef](#)]
12. Daissaoui, A.; Boulmakoul, A.; Karim, L.; Lbath, A. IoT and Big Data Analytics for Smart Buildings: A Survey. *Procedia Comput. Sci.* **2020**, *170*, 161–168. [[CrossRef](#)]
13. Kim, Y.; Park, Y.; Choi, J. A study on the adoption of IoT smart home service: Using value-based adoption model. *Total Qual. Manag. Bus. Excell.* **2017**, *28*, 1149–1165. [[CrossRef](#)]
14. Dreyer, S.; Olivotti, D.; Lebek, B.; Breitner, M.H. Focusing the customer through smart service: A literature review. *Electr. Mark.* **2019**, *29*, 55–78. [[CrossRef](#)]
15. Zhang, N.; Mi, X.; Feng, X.; Wang, X.F.; Tian, Y.; Qian, F. Understanding and mitigating the security risks of voice-controlled third-party skills on amazon alexa and google home. *arXiv* **2018**, arXiv:1805.01525.
16. Benmansour, A.; Bouchachia, A.; Feham, M. Multioccupant Activity Recognition in Pervasive Smart Home Environments. *ACM Comput. Surv.* **2016**, *48*, 1–36. [[CrossRef](#)]
17. Russell, L.; Goubran, R.; Kwamena, F. Personalization Using Sensors for Preliminary Human Detection in an IoT Environment. In Proceedings of the 2015 International Conference on Distributed Computing in Sensor Systems, Fortaleza, Brazil, 10–12 June 2015; pp. 236–241.
18. Majumder, S.; Aghayi, E.; Noferesti, M.; Memarzadeh-Tehran, H.; Mondal, T.; Pang, Z.; Deen, M.J. Smart Homes for Elderly Healthcare—Recent Advances and Research Challenges. *Sensors* **2017**, *17*, 2496. [[CrossRef](#)]
19. Alrawi, O.; Lever, C.; Antonakakis, M.; Monroe, F. Sok: Security Evaluation of Home-based IoT Deployments. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), San Francisco, CA, USA, 20–22 May 2019.
20. Triyono, L.; Yudiantoro, T.R.; Sukanto, S.; Hestiningih, I. VeRO: Smart home assistant for blind with voice recognition. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1108*, 012016. [[CrossRef](#)]
21. Kim, S. Exploring How Older Adults Use a Smart Speaker-Based Voice Assistant in Their First Interactions: Qualitative Study. *JMIR Mhealth Uhealth* **2021**, *9*, e20427. [[CrossRef](#)]
22. Abdi, N.; Zhan, X.; Ramokapane, K.M.; Such, J. Privacy Norms for Smart Home Personal Assistants. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2021.
23. Kushalnagar, N.; Montenegro, G.; Schumacher, C. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*; IETF Trust: Fremont, CA, USA, 2007.
24. Chávez-Santiago, R.; Szydelko, M.; Kliks, A.; Foukalas, F.; Haddad, Y.; Nolan, K.E.; Kelly, M.Y.; Masonta, M.T.; Balasingham, I. 5G: The Convergence of Wireless Communications. *Wirel. Pers. Commun.* **2015**, *83*, 1617–1642. [[CrossRef](#)]
25. Costanzo, A.; Masotti, D. Energizing 5G: Near- and Far-Field Wireless Energy and Data Transfer as an Enabling Technology for the 5G IoT. *IEEE Microw. Mag.* **2017**, *18*, 125–136. [[CrossRef](#)]
26. Kobo, H.I.; Abu-Mahfouz, A.; Hancke, G.P. A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements. *IEEE Access* **2017**, *5*, 1872–1899. [[CrossRef](#)]
27. Qiu, W.; Saleem, K.; Pham, M.; Halpern, M.; Beresford-Smith, B.; Overmars, A.; Dassanayake, K.; Thoms, G. Robust Multipath Links for Wireless Sensor Networks in Irrigation Applications. In Proceedings of the 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, Melbourne, Australia, 25 April 2008; pp. 95–100.
28. Overmars, A.; Venkatraman, S. Towards a Secure and Scalable IoT Infrastructure: A Pilot Deployment for a Smart Water Monitoring System. *Technologies* **2020**, *8*, 50. [[CrossRef](#)]
29. Coucke, A.; Saade, A.; Ball, A.; Bluche, T.; Caulier, A.; Leroy, D.; Doumouro, C.; Gisselbrecht, T.; Caltagirone, F.; Lavril, T.; et al. Snips voice platform: An embedded spoken language understanding system for private-by-design voice interfaces. *arXiv* **2018**, arXiv:1805.10190.
30. Hoy, M.B. Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. *Med. Ref. Serv. Q.* **2018**, *37*, 81–88. [[CrossRef](#)]
31. Guamán, S.; Calvopiña, A.; Orta, P.; Tapia Leon, F.; Yoo, S.G. Device Control System for a Smart Home using Voice Commands: A Practical Case. In Proceedings of the 2018 10th International Conference on Information Management and Engineering, Manchester, UK, 22–24 September 2018; pp. 86–89.
32. Moorthy, A.E.; Vu, L. Privacy concerns for use of voice activated personal assistant in the public space. *Int. J. Hum. Comput. Interact.* **2015**, *31*, 307–335. [[CrossRef](#)]

33. Humphry, J.; Chesher, C. Preparing for smart voice assistants: Cultural histories and media innovations. *New Media Soc.* **2020**, *23*, 1971–1988. [[CrossRef](#)]
34. Liu, Y.; Gan, Y.; Song, Y.; Liu, J. What Influences the Perceived Trust of a Voice-Enabled Smart Home System: An Empirical Study. *Sensors* **2021**, *21*, 2037. [[CrossRef](#)] [[PubMed](#)]
35. Lau, J.; Zimmerman, B.; Schaub, F. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In Proceedings of the ACM on Human-Computer Interaction, Palma, Spain, 12–14 September 2018.
36. Apthorpe, N.; Reisman, D.; Sundaresan, S.; Narayanan, A.; Feamster, N. Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic. *arXiv* **2017**, arXiv:1708.05044.
37. Singh, J.; Pasquier, T.; Bacon, J.; Ko, H.; Eysers, D. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet Things J.* **2015**, *3*, 269–284. [[CrossRef](#)]
38. Ntuli, N.; Abu-Mahfouz, A. A Simple Security Architecture for Smart Water Management System. *Procedia Comput. Sci.* **2016**, *83*, 1164–1169. [[CrossRef](#)]
39. Venkatraman, S.; Overmars, A. New Method of Prime Factorisation-Based Attacks on RSA Authentication in IoT. *Cryptography* **2019**, *3*, 20. [[CrossRef](#)]
40. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [[CrossRef](#)]
41. El-Azab, R. Smart homes: Potentials and challenges. *Clean Energy* **2021**, *5*, 302–315. [[CrossRef](#)]
42. Pira, S. The social issues of smart home: A review of four European cities' experiences. *Eur. J. Futur. Res.* **2021**, *9*, 1–15. [[CrossRef](#)]