

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository:<https://orca.cardiff.ac.uk/id/eprint/177336/>

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Dodd, Callum, Saxena, Neetesh and Maity 2025. Security analysis of smart home devices: Smart life and Philip Hue. Presented at: IEEE PerCom - International Workshop on Security, Privacy and Trust in the Internet of Things (SPT-IoT), Washington, USA, 17-21 March 2025. 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops). IEEE, pp. 398-403. 10.1109/PerComWorkshops65533.2025.00098

Publishers page: [https://doi.org/ 10.1109/PerComWorkshops65533.2025...](https://doi.org/10.1109/PerComWorkshops65533.2025...)

Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See <http://orca.cf.ac.uk/policies.html> for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.



Security Analysis of Smart Home Devices: Smart Life and Philip Hue

Callum Jack Dodd

Digital Trust and Cyber Security
PA Consulting
London, United Kingdom
i7463698@bournemouth.ac.uk

Neetesh Saxena

School of Computer Science and Informatics
Cardiff University
Cardiff, United Kingdom
nsaxena@ieee.org

Soumyadev Maity

Department of Information Technology
IIIT Allahabad
Prayagraj, India
soumyadev@iiita.ac.in

Abstract—Security of smart home devices has become paramount as these devices are now more popular in households and have started to play a major role in our daily lives. In this work, we looked into the security aspect of smart home devices by exploring their security mechanisms, and adverse impact when comprising and identifying end-user knowledge and technical requirements for securing Smart Home networks. We performed a penetration test to identify vulnerabilities within two main Smart Home apps (Smart Life and Philip Hue). During our analysis and evaluation, we found that these devices are insecure and have security vulnerabilities of defaulted passwords, unauthorised users on the Smart Home network and key data being transmitted in clear text. We further designed and implemented a solution for minimising such vulnerabilities.

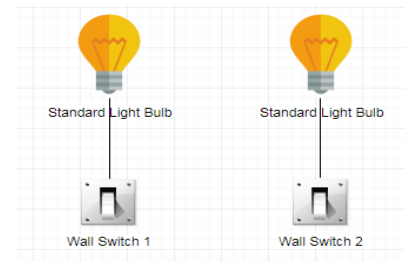
Index Terms—smart home devices, security, default passwords, unauthorised users.

I. INTRODUCTION

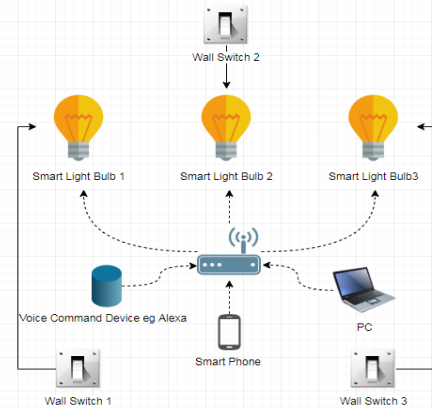
Internet of Things (IoT) - Smart Home Devices (SHDs) are becoming more popular in households due to their ease of use, energy efficiency, and ability to become more automated. With a 135% year on year increase in Smart Home Device sales, they are the latest household accessory [1]. 51% of consumers had bought a smart home device to help adapt to pandemic living [2]. These smart devices have functions ranging from playing music, turning on plugs, or even ordering washing powder before it runs out. As smart home devices become more popular, even being installed in new cars, it begs the question of how secure our personal data is. With 55% of Smart Home Device consumers admitting they do not fully understand the security within these devices [3], and their personal data being put at risk for the benefit of a more convenient way of controlling these devices.

The effectiveness of smart home devices can be seen when a standard light bulb is compared to a smart light bulb. Figure 1 illustrates the functioning of standard and smart light bulbs. A standard light bulb is connected to a minimum of one wall switch, and in some cases can be connected to two wall switches. On average these light bulbs provide an output of 28 watts. However, a smart light bulb is not only cheaper to run, with an average output of only 10 watts (Philips Hue), but it also provides an easier and a remote way of turning on and off. An IoT setup for smart light bulbs could allow the

Identify applicable funding agency here. If none, delete this.



(a) Standard light bulb connecting scenario.



(b) Smart light bulb connecting scenario.

Fig. 1: Standard light vs. smart light bulb setup.

user to control the light via voice commands, a smart phone, a PC, motion sensors, or a standard wall switch.

Although IoT devices are becoming more popular, the security of these devices has not been implemented to a high standard. Smart home devices communicate with one another via a Local Area Network (LAN). Normally, for security reasons, most of the traffic on a LAN is encrypted. However, in the case of many smart home devices, the traffic has not been encrypted. In some cases, even in devices that have encryption, the secret key is in the public domain making the encryption invalid. This poses a major security threat allowing unauthorised users to intercept packets, passwords, and even access personal data. With an increasing number of cyber-attacks on IoT devices, it is important to ensure that personal

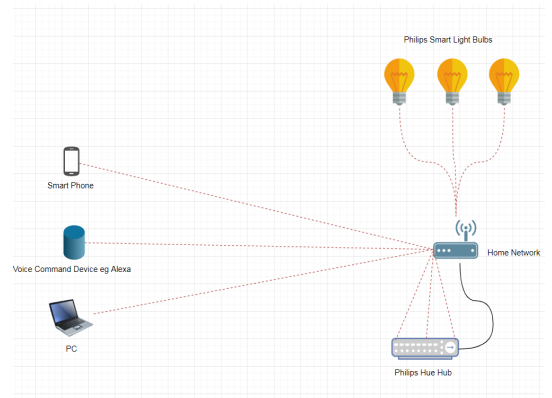
data is secure and cannot be intercepted, decrypted, or spied upon. These attacks could range from exploiting household lights accessing to a home network and data, including emails. Manufacturers have been aware of security issues and have released updated version of such devices claiming to have fixed the problems. However, this has proved to be incorrect on several instances. The security of IoT smart home devices has yet to improve to a level where data is secure from cyber-attacks.

This work analyses the vulnerabilities of smart home devices, looking for potential threats that could be exploited. We summarise our contributions as follows.

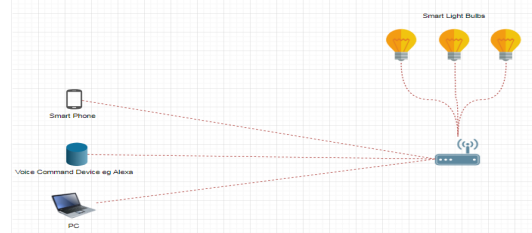
- Analysed vulnerabilities of smart home devices and explored research gaps.
- Experimented and conducted an attack on Philips Smart Light to exploit vulnerability to show real-life impact.
- Designed and implemented a secure solution via an app for home users.

II. RELATED WORK

Vulnerabilities have been identified in over 40% of smart home devices [1]. Smart home devices interact with the smart app called ‘Smart Life’. Some of the manufactures of such devices are Anhome, Oitmm Smart and Jinvoov Smart. Philips was one of the first companies to launch smart home devices, the smart light bulb in 2012. The device had a vulnerability allowing hackers to gain access to users’ smart home networks, and exploit their wireless smart home devices [4]. A demonstration of how vulnerabilities could be exploited in smart light bulbs was published in 2016 [5]. It showed a drone taking control of smart light bulbs in an office building. This vulnerability was due to a component within the bulb, which allowed unauthorised users to take control of all smart light bulbs. Generation 2 of Philips smart light bulb was released in 2015, claiming to have fixed the issues of unauthorised users gaining access, and Generation 3 was released in 2016. However, with smart home devices becoming ever more popular, it has become apparent that these companies as a whole have not invested enough into the security of these devices. Existing research in this area proposed frameworks [6], ranking security of IoT devices [7], and study risk and vulnerabilities in smart devices [8],[9], for evaluating security and privacy of the smart home devices, however, there is only single work available exploring and exploiting smart bulb vulnerabilities for TP-Link smart bulb [10], which is from a different manufacturer than the devices considered in this work. Therefore, we investigated the security vulnerability in this work. Throughout this research, multiple vulnerabilities have been identified. These vulnerabilities include default encryption passwords being transmitted in clear text, default passwords in the public domain and an inability to change passwords. Although some of these vulnerabilities may not seem important currently, they could have a major impact in the near future. With companies like Philips incorporating smart light bulbs in streetlights, office buildings and other areas



(a) External hub layout (hub required layout).



(b) Router hub layout (Non-hub requirement).

Fig. 2: Connecting hub layout for the setup.

of public interest, such vulnerabilities could lead to blackouts not only in homes but also on the streets or at places of work.

Vulnerabilities lie in many different types of smart home devices. The main types of known vulnerabilities are: default password, password transmitted in the clear, lack of authentication, and lack of encryption. It is important to point out that not all smart home devices may have these vulnerabilities; however, these are identified as the most common ones. Whether smart home devices use the router as a hub or have an external hub, there are vulnerabilities that could allow an attacker to gain access to them. Hackers could intercept packets and use them to take advantage. Although smart home devices have been around for the past few years, the poor security of these devices is still allowing attackers to gain access to them. Further, existing solutions suggested how to fix any security issues related to authentication such as in [11], [12], and [13]. Alharbi and Aspinall [11] suggested encrypting all data transmitted so that anyone sniffing the traffic will not get vital information. However, this cannot be done without the manufacturer or need to deploy over an app hub or smart device itself. Kim [12] proposed to add authentication to authorise new users so that the main user will be able to see who has access and give access to whom they wish. Rehman and Gruhn [13] proposed to implement a Firewall but more likely this will prevent external attackers and less likely to stop internal attackers from exploiting the system. Note that changing default passwords and username will not help here, as sniffing on the network may still see the new passwords and/or username. We developed an app/prototype to provide secure authentication to the home users.

III. SYSTEM AND ATTACK MODEL

This section explores a system model and possible attack scenario that may occur with the current layout and security of the Philips Hue smart home device. There are two ways that smart home devices can operate. The first uses the home router as the hub and connects directly to the router, as shown in Figure 2. The second uses a hub that is connected to the router and directs the packets. For some devices, the Alexa Plus or the Philips Hue hub can be used. Whether a smart home device uses an external hub or the router as the hub, it uses the IEEE 802.15.4 bridge to communicate via the control devices (phone, PC or voice) and the smart home devices. The IEEE 802.15.4 is a technical standard that defines how the operations of Low Rate Wireless Personal Area Networks (LR-WPANs) should behave. ZigBee is also used within smart home devices as it is small, has low power usage, and uses low data rate. ZigBee works with the IEEE 802.15.4 to transmit data via a 2.4GHz radio band either as Wi-Fi or Bluetooth.

Consider a scenario where an organisation has recently installed new light bulbs throughout the office building. The organisation decides to upgrade their current light bulbs to smart bulbs, because they are, on average, cheaper to run and all company's lights will be controlled from one device. The smart light bulbs are running on their current wireless network, just like all the other computers within the organisation. A misuse case has been created in Figure 3, showing how an attacker could gain access to the office smart lights. The blue lines show the authorised communication between the authorised user and the smart lights. The red lines show how an attacker could exploit the smart home devices by authenticating their devices with the hub in order to take control of the smart lights. As described in the next section, the attacker could use the scripts that we created to generate a secret key and become authorised to take control of the smart lights. The attack tree in Figure 4 shows the steps taken to carry out this misuse case. This reflects the steps the hacker would have to take to gain access to the hub, and the types of attack that could be carried out once access has been gained.

IV. OUR APPROACH AND ANALYSIS

This section analyses smart home devices and exploring vulnerabilities and proposes a secure solution. The analysis focuses on the two main apps used for controlling smart home devices: 'Smart Life' and 'Philips Hue'. The analysis of smart home devices has been broken down into two sections. The analysis will look at both the Smart Life app and the Philips Hue app, as both are among the most used apps for smart home devices.

A. Analysis of Smart Life App

The Smart Life app works with a range of different types of manufacturer, some of which are Anhome, Oitmm Smart and Jinvoov Smart. Before the advent of Smart Life, multiple different apps were needed to control smart home devices.

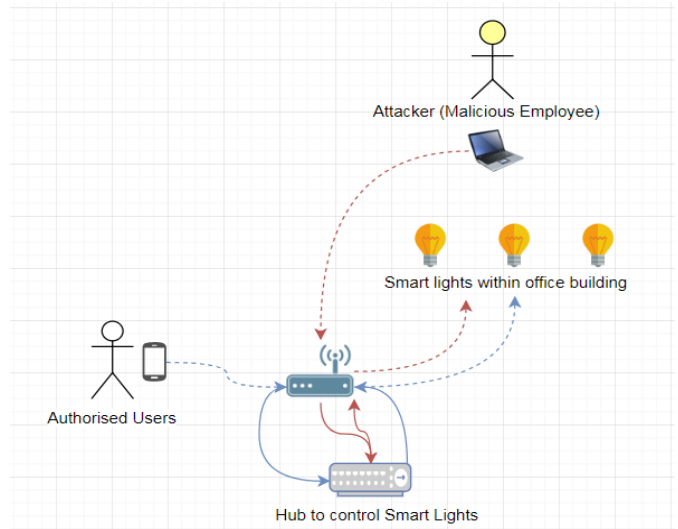


Fig. 3: Misuse Case.

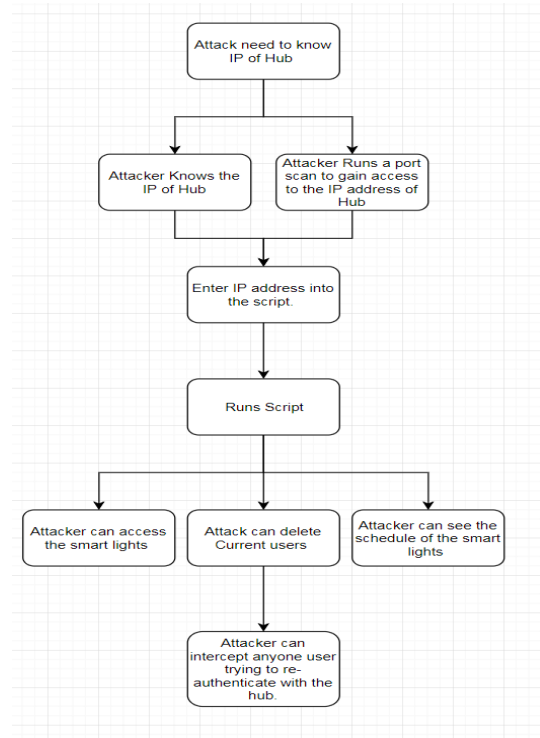


Fig. 4: Attack Tree for Philip Hue.

However, now all devices can be connected to one app, which works without an external hub, and can control a range of different devices. As long as the appliances like bread makers, gas stoves, plugs or lights are smart home devices, the app can control them. The focus of the analysis of the Smart Life app and devices is on smart plugs and smart light bulbs, manufactured by Austein and Slitinto.

1) *Potential Vulnerability: Control App to Smart Device Communication:* To analyse the data being transmitted between the control device (smart phone) and the Smart Home

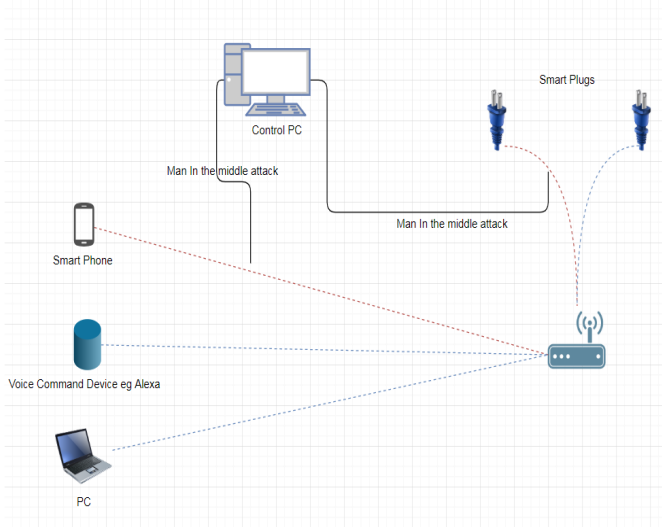


Fig. 5: Testing Environment for Smart Life.

```

Client ID Length: 20
Client ID: 1274756684f3ebb8a18f
Will Topic Length: 15
Will Topic: tuja/smart/will
Will Message Length: 107
Will Message: {"clientId":"1274756684f3ebb8a18f","deviceType":"GATEWAY","message":"11","userName":"1274756684f3ebb8a18f"}
User Name Length: 20
User Name: 1274756684f3ebb8a18f
Password Length: 16
Password: bdc0fa86435dbd05

```

Fig. 6: Format of the data in packets.

Device (smart plugs), a testing environment is created, which is shown in Figure 5.

The red lines show the traffic of the data being transmitted when using Wireshark to capture the data. The blue lines are other ways that could communicate with the smart home devices. To gain access to the traffic, the control PC performed a Man-in-the-Middle (MITM) attack. This attack allowed the control PC to gain access to packets being transmitted between the two devices. After conducting a MITM attack, the packets transmitted are analysed using Wireshark.

A format of the packet carrying the transmitted data is shown in Figure 6. It can be observed that the packet transmitted the username and password in clear text. An attacker can gain access to smart home devices through this weak security control. Another interesting discovery is to see the device talking to an external server, 25.28.217.66, as it could lead to other vulnerabilities to disrupt the ability of a user to control their Smart Home Device(s). Access to the server address enabled discovery of the location of the server and to whom it belongs. For the information, this server belonged to Amazon and was located in Germany (Db-ip.com).

2) *Exploiting the Vulnerability and Recommendation:* From the observation of our experiment, there are two main vulnerabilities that an attacker could exploit. The first and most important attack would be to use the username and password to gain access to the smart home device(s). Having gained

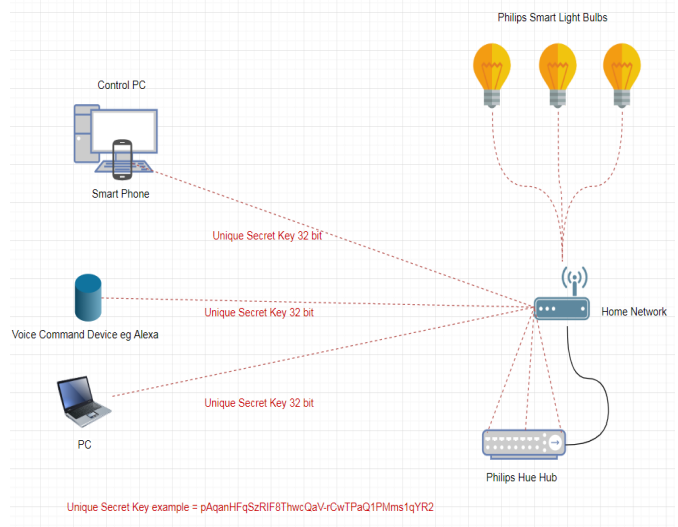


Fig. 7: Test Environment for Philips Hue.

access to the device, the attacker could then start exploiting the vulnerability. An attack could range from turning on a light to controlling the house heating. This would depend on the devices that have been accessed. The other attack a hacker might exploit is an attack on the server with which the devices are communicating (52.58.217.66). The hacker could perform a Denial of Service attack (DoS), thereby denying the users the use of the server.

As our recommendation, the best solution for this vulnerability is to add encryption to the communication of these packets. This could be accomplished by transmitting the data using Transport Layer Security (TLS)v1.3 protocol. Adding TLS would provide a layer of security to the traffic, preventing anyone sniffing the traffic gaining access to data, without knowing the ciphers for the transmitted data.

B. Analysis of Philips Hue App

The Philips Hue app is among the most popular app and manufacture of smart home devices. To analyse these devices, both, the data being transmitted between the command device (Phone app and Amazon Alexa) to the hub and the data being transmitted between the hub and the devices, are studied.

1) *Evaluating Potential Vulnerability- Hub to Device Communication:* To identify possible vulnerabilities, a controlled environment is created in which a control PC would be able to intercept all the packets using Wireshark, as shown in Figure 7. The vulnerability found was within the Philips Hue Hub that allowed an attacker to gain access to the Hub. When capturing packets between the different devices (the smart phone to the Philips Hue hub, and the Philips Hue hub to the Philips Smart Light Bulb), port mirroring is also set up. Port mirroring allowed all the packets being transmitted between different devices to also be transmitted to the Control PC. In this way, the packets could be analysed and an attack script is created. In this case, the smart phone was an emulator running on a Virtual Machine on the control PC.

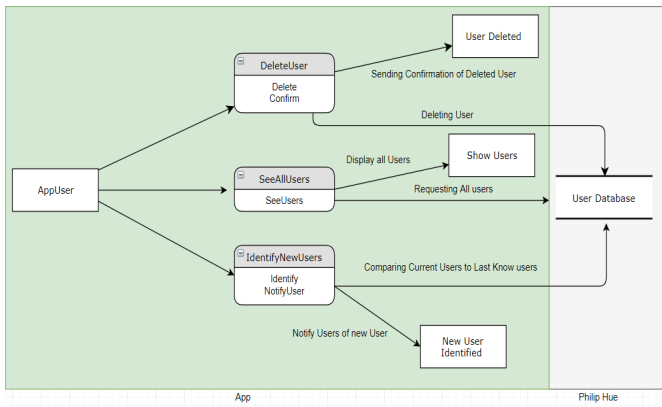


Fig. 10: High Level Data Flow.

on the hub network. This is what the below script shows. This script requests a ‘secret key’ from the hub, which then gets saved in a text file. This text file is then used with the ‘secret key’ for the other scripts.

Identifying Current Users: To be able to identify new user, a script has been created. This script reads in a hub key that has been created from the above script, authenticating app with hub. This script will then gather the data from the hub and save it in a text file called ‘Current Users’.

Deleting Users: The ‘deleting user’ script relies on two other text files. The first text file is ‘AppKey’. This is generated and saved as a text file from the first script ‘Authenticating App with Hub’. The second text file needed for this script is the user ID of the soon to be deleted user. This text file is created and saved as a text file when the user enters in the ID from the user interface. With both the text file, the app sends a message to the hub such as; ‘(AppKey.txt)/config/whitelist/(DeletedUsers)’. This command instructs the hub to delete that user.

3) *GUI to Control Script:* Having created the above scripts, a control user interface is needed to control each script. Figure 19 shows the developed prototype, i.e., App. This is where the user will be able to navigate and communicate with the hub.

V. CONCLUSION

The aim of this work was to show how secure smart home devices are and to look at solutions to advance their security. We conducted research to explore known vulnerabilities of all types of smart home devices. This has identified the main vulnerabilities as unauthorised access, data transmitted in clear text, and little to no encryption of data. Having identified these vulnerabilities a test environment was set up to analyse the two main smart home devices apps: Philips Hue and Smart Life. It was decided to implement the addition of authentication to the Philips Hue hub. This implementation allows the main user of Philips Hue to delete unwanted users from their Smart Home network. This work has identified a key issue, which is that the Smart Life app transmits the username and passwords in clear text. This can allow an attacker to snoop the network traffic and intercept data. Smart Life works with a range of different Smart Home Device manufacturers, which

means that this vulnerability is deeply embedded. This work also focused on creating and implementing a solution to the vulnerabilities of the Philips Hue hub. The work focused on this manufacturer because of the critical findings that were highlighted during the research stage. The Key Findings for Philips Hue: unauthorised users can gain access to the Philips Hue hub; unauthorised users can snoop network traffic to find the ‘Secret Key’; attackers can delete authorised users from the hub, which authorised users cannot do via the app; and attackers can gain access to the schedules of the smart home devices – attackers can delete or edit the schedules.

The above findings have shown that the Philips Hue hub is open to attack from both internal and external attackers. The attacker has the ability, with the above vulnerabilities, to access the Smart Home network, take control of the smart home devices, delete authorised users and change the schedule. These vulnerabilities could allow an attacker to gain access and lock legitimate users out of their smart home devices.

ACKNOWLEDGMENTS

This work was supported by the UKIERI via British Council (UK), Research Institute In Trustworthy Inter-Connected Cyber-Physical Systems (RITICS), United Kingdom, and Google Research.

REFERENCES

- [1] S. Gatlan, “Smart Homes at Risk Due to Unpatched Vulnerabilities, Weak Credentials,” *BleepingComputer*, 2019.
- [2] R. Daws, “Pan(ic)demic buying: 51% of consumers bought a smart home device,” *IoTNews*, 2021. <https://iottechnews.com/news/panicdemic-buying-51-consumers-bought-smart-home-device/>.
- [3] Elssolutions, 2024. The Future of Smart Home Technology in the UK. <https://ecelectronics.com/news/the-future-of-smart-home-technology-in-the-uk>
- [4] CVE-2024-9991, Jun 2024. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-9991>.
- [5] D. Storm, “Researchers hack Philips Hue lights via a drone; IoT worm could cause city blackout,” *Computerworld*, 2016. <https://www.computerworld.com/article/3139860/researchers-hack-philips-hue-lights-via-a-drone-iot-worm-could-cause-city-blackout.html> [Accessed 26 Feb. 2019].
- [6] R. Mangar, T. J. Pierson and D. Kotz, “A Framework for Evaluating the Security and Privacy of Smart-Home Devices, and its Application to Common Platforms,” in *IEEE Pervasive Computing*, vol. 23, no. 3, pp. 7-19, July-Sept. 2024.
- [7] N. M. Allifan and I. A. Zuakernan, “Ranking Security of IoT-Based Smart Home Consumer Devices,” in *IEEE Access*, vol. 10, pp. 18352-18369, 2022.
- [8] X. Chen, C. Yang, Y. Nan and Z. Zheng, “An Empirical Study of High-Risk Vulnerabilities in IoT Systems,” in *IEEE Internet of Things Journal*, 2024.
- [9] A. Sedighfar, “A Study on Smart Homes Vulnerabilities,” 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 2024, pp. 117-122.
- [10] D. Bonaventura, S. Esposito, and G. Bella, “Smart Bulbs Can Be Hacked to Hack into Your Household,” 20th International Conference on Security and Cryptography, 2023, pp. 218-229.
- [11] R. Alharbi and D. Aspinall, “An IoT analysis framework: An investigation of IoT smart cameras’ vulnerabilities,” *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, 2018, pp. 1-10.
- [12] J. T. Kim, “Analyses of secure authentication scheme for smart home system based on internet on things,” 2017 International Conference on Applied System Innovation (ICASI), Sapporo, Japan, 2017, pp. 335-336.
- [13] S. Rehman and V. Gruhn, “An approach to secure smart homes in cyber-physical systems/Internet-of-Things,” *Fifth International Conference on Software Defined Systems (SDS)*, Barcelona, Spain, 2018, pp. 126-129.