**Borneo International Journal eISSN 2636-9826**; Vol. 7 (2); 2024; 1-11
Published by *Majmuah Enterprise*
www.majmuah.com

# A Preliminary Analysis of Bluetooth and Wi-Fi Security in Residential IoT Ecosystems

AZRAN ABDUL RAZAK
Jabatan Teknologi Maklumat dan Komunikasi (JTMK), Politeknik Tuanku Syed Sirajuddin (PTSS),
Arau, Perlis, Malaysia

Email:azranar@ptss.edu.my

MOHAMAD FADLI ZOLKIPLI
School of Computing, College of Arts and Sciences Universiti Utara Malaysia
Sintok, Kedah, Malaysia

Email: mzulhelmin@utm.my

Received: April 01, 2024
Accepted: May 01, 2024
Online Published: June 04, 2024

**Abstract**

In the context of residential IoT ecosystems, the paper explores the security landscape of popular communication protocols, including Bluetooth and Wi-Fi. The research attempts to uncover possible hazards, weaknesses, and concerns related to the adoption of IoT devices in home settings that use various communication protocols through a methodical process. Authentication methods, encryption techniques, and the general strength of security features in widely used smart devices are important areas of study. The results of the investigation highlight how urgently enhanced security measures are needed in the quickly developing field of residential Internet of Things (IoT) systems. Expanding on knowledge from earlier studies on IoT vulnerabilities, protecting consumer environments demands a comprehensive approach. Prospects could assist with creating a smart home environment that is safer and more reliable by implementing the recommendations made by the researchers into the implementation and use of IoT devices in the residential area. Protecting the interconnected structure of residential IoT ecosystems requires proactive measures and properly educated decision-making, as the field of Internet of Things (IoT) security continues to grow.

**Keywords**: Wi-fi, Bluetooth; Internet of Things

## 1. Introduction

The continuous introduction of new gadgets into networks is a defining feature of the Internet of Things' (IoT) explosive growth. Improved communication, automated procedures, and improved monitoring are just a few benefits of connectedness. However, the advantages come with a risk. Network accessibility creates new attack avenues for Internet of Things devices. Unfortunately, many of home appliances that are connected to the internet have wireless communication risks and poor cyber security requirements. The primary goal of this journal is to do a preliminary analysis of Bluetooth and Wi-Fi security issues in the environment of residential Internet of Things (IoT) systems. As Internet of Things (IoT) gadgets become increasingly popular in homes, worries about possible security flaws in widely used communication protocols like Bluetooth and Wi-Fi connection grow. With two such significant points of entry point, an attacker can quickly take advantage of a weakness to get in and harm the victim. According to (Nor Naematul Saadah and Mohamad Fadli 2023) common user of these devices is concerned because of the internet of things' vulnerability to cyberattacks because of their unique characteristics and weak configurations.

## 2. Literature review

IoT devices have traditionally relied on Bluetooth and Wi-Fi as their core communication methods. These technologies offer seamless communication but also carry some risk. As these technologies have developed, the number of linked devices has increased, raising issues with encryption, authentication, and general security. Previous studies draw attention to problems like shoddy authentication procedures, vulnerability to listening in on conversations, and the possibility of unwanted access. Furthermore, the history of IoT device security problems highlights the importance it is to fix these vulnerabilities. The cybersecurity community is concerned about threats such device hijacking, data breaches, and the use of unsafe communication methods. The current investigation, which attempts to systematically

explore the security implications of Bluetooth- and Wi-Fi-enabled Internet of Things (IoT) gadgets in home contexts, will not be possible without an understanding of this past.

## 3. Existing Security Attack Type on Popular IoT Environment

**Table 1** : Attack type targeting IoT devices based on their respective attack types, protocols, and descriptions.

| Attack Type | Protocol | Description |
|---|---|---|
| Rogue Device Connections | Wi-Fi | Attackers set up rogue Wi-Fi access points to trick IoT devices into connecting to them, exposing them to risks. |
| | Bluetooth | Attackers impersonate legitimate Bluetooth devices to establish unauthorized connections. |
| Firmware Exploitation | Wi-Fi | Vulnerabilities in firmware may be exploited to gain control over the device or install malicious software. |
| | Bluetooth | Similar to Wi-Fi, vulnerabilities in firmware can be exploited to manipulate device functions or install malware. |
| Zero-Day Exploits | Wi-Fi | Attacks targeting unknown vulnerabilities in protocols or software can pose a significant threat until patched. |
| | Bluetooth | Zero-day exploits in Bluetooth protocols or software can also pose significant threats until patches are released. |
| Eavesdropping | Wi-Fi | Unsecured channels can be exploited to eavesdrop on sensitive information transmitted between devices and networks. |
| | Bluetooth | Similar to Wi-Fi, unsecured channels in Bluetooth can be exploited for eavesdropping on sensitive information. |
| Man-in-the-Middle Attacks | Wi-Fi | Attackers intercept and alter communication between the IoT device and network, leading to unauthorized access. |
| | Bluetooth | Attackers intercept Bluetooth communication, allowing for eavesdropping or injection of malicious data. |
| Denial-of-Service Attacks | Wi-Fi | Overloading Wi-Fi networks with excessive requests can disrupt service for IoT devices. |
| | Bluetooth | Jamming Bluetooth frequencies can disrupt device communication, rendering them unable to communicate effectively. |
| Bluejacking and Bluesnarfing | Bluetooth | Bluejacking involves sending unsolicited messages, while bluesnarfing targets unauthorized access to device data. |
| Credential Attacks | Wi-Fi | Brute-force attacks or credential interception can compromise device security, allowing unauthorized access. |
| | Bluetooth | Similar to Wi-Fi, credential attacks can compromise Bluetooth device security, leading to unauthorized access. |

This table organizes the different hacking techniques targeting IoT devices based on their respective attack types, protocols, and descriptions. Overall, the table serves as a valuable reference for understanding the landscape of IoT security threats and the techniques used by attackers to exploit vulnerabilities in Wi-Fi and Bluetooth-enabled IOT devices. DoS attacks pose a serious risk to household IoT devices. According to (Ariyadi and Pohan 2023) all connected devices to the Wi-Fi network become disconnected and unable to reconnect as a result of denial-of-service attacks. The attack may interfere with smart home systems, which could be harmful and inconvenient to user.

According to (Fatima, Khan, and Akbar 2021) considering they are simpler to remember, many people choose comfort over security and employ simple password patterns rather than complicated ones. Once the user has used a basic password, attackers can quickly guess the username and password by attempting every possible combination (i.e., using "brute force") until they find one that matches. It happens in both Bluetooth and WiFi scenarios during a credit attack.

**Figure 1***:* Digital harms identified for each smart home device.

| | Privacy intrusion | Hacking | Malware | DoS | Stalking |
|---|---|---|---|---|---|
| Security and surveillance | 10 | 9 | 7 | 12 | 2 |
| Lighting control, smart bulb | 7 | 12 | 9 | 9 | 1 |
| Voice control device | 7 | 10 | 4 | 5 | 1 |
| Temperature and ventilation | 4 | 6 | 6 | 5 | 3 |
| Smart home app or browser | 4 | 7 | 6 | 3 | 1 |
| Occupancy-aware control | 4 | 6 | 6 | 5 | 1 |
| Smart plug | 5 | 8 | 5 | 4 | 1 |
| Automation for elderly/sick | 7 | 2 | 1 | 1 | 1 |
| Entertainment | 2 | 3 | 5 | 5 | 2 |
| WiFi | 2 | 4 | 1 | 5 | 0 |
| Smart kitchen | 0 | 4 | 3 | 1 | 0 |
| Smart grid and smart meter | 3 | 0 | 0 | 0 | 0 |
| Leak detector and air quality | 1 | 2 | 2 | 2 | 1 |
| Pet or baby care | 1 | 1 | 1 | 2 | 0 |
| Cleaning robot | 1 | 1 | 0 | 1 | 0 |

Additionally, according (Buil- Gil et al., 2023) researchers documented the kinds of data that provide digital harms in each scenario as well as the digital harms that were detected for various kinds of smart home devices refer Figure 1. In analysing the data, it becomes evident that security and surveillance devices face the highest risk of hacking, followed by Wi-Fi-connected devices, with cleaning robots appearing to have the least vulnerability. Since all these devices rely on either Wi-Fi or Bluetooth for communication with users, it is advisable for consumers to conduct thorough research on brands and products in the current market, considering their historical vulnerability to security breaches in Wi-Fi and Bluetooth communication protocols.

According to (Heiding et al. 2023) perform testing on 22 devices found 17 vulnerabilities, which were then released as new Common flaws and Exposures (CVEs). The operation and integrity of smart home systems could be jeopardized by attackers thanks to these vulnerabilities, which represent serious dangers to the security of IoT home services. The tested gadgets are sold to private persons globally, which emphasizes how critical it is to fix these vulnerabilities to protect IoT home users' privacy and safety.

**Vulnerabilities in Wireless Protocol Versions**

**Table 2** : Attack types, protocols targeted, descriptions of vulnerabilities, and the tools/methods used to exploit them.

| Attack Type | Protocol | Description | Tools/Methods Used |
|---|---|---|---|
| Attacking WEP | Wi-Fi | WEP is vulnerable to brute-force attacks and can be compromised within minutes using tools like Aircrack. | Aircrack |
| Attacking WPA2 | Wi-Fi | WPA2 can be targeted through brute forcing WPS PIN, similar to WPA attacks, with tools like Reaver. | Reaver |

According to researchers (Ahmed Adbeib 2023) successfully conducted experiments testing the cracking of protocols as outlined in the table. This highlights the critical need for IoT product manufacturers to address vulnerabilities in Wi-Fi protocols, such as WEP and WPA2, as demonstrated by the ease with which these protocols can be compromised using readily available tools like Aircrack and Reaver. Failure to address these vulnerabilities can expose IoT devices to potential security breaches, compromising user privacy and data integrity. Several risks exist for ZigBee device, a wireless communication technology that is frequently used in Internet of Things devices for low-power, short-range communication. According to (Sadikin et al. 2023) the attack scenario by ZigBee include reconnaissance, in which

hostile parties get information about prospective strikes, denial-of-service (DoS), which attempts to interfere with system operations, device hijacking, which is the illegal takeover of legitimate devices to prevent authorized users from using them and malicious control, which is accomplished by posing as trustworthy devices for unauthorized usage.

In addition to agricultural applications, similar challenges are encountered in home IoT gardens. According to (Rudrakar and Rughani 2023) apart from overseeing and managing sensors, the agri-sector's low-power wireless networks, like LoRaWAN and Zigbee, are susceptible to adverse environmental factors like temperature, humidity, obstructions, and human activity. These factors can consequently interfere with communication and cause data loss. This could lead to inaccurate data processing and faulty functioning of the smart farm system.

**Table 3** : Overview of each software tool's functionality and its purpose in experimenting with hacking the Tapo C200 IoT camera.

| Software Tool | Functionality | Purpose in Experimenting with Tapo C200 IoT Camera |
|---|---|---|
| Ettercap | Man-in-the-Middle attack toolkit; breaks apart protocols, filters contents, and captures network packets | Listen in on conversations between the Tapo camera and its application |
| Nessus | Vulnerability scanner; evaluates overall security against known threats and weaknesses | Evaluate the Tapo camera's vulnerabilities |
| Nmap | Network discovery tool: quickly scans networks to find active hosts and services | Collect data regarding the services exposed by the Tapo camera |
| SSL Packet Capture | Powerful debugging tool: intercepts encrypted data for further examination | Decipher SSL communications to and from the Tapo application |
| Iptables | Administration tool for NAT and packet filtering; manages firewall rules within Linux kernel | Act as an active mediator between the Tapo camera and its application, controlling network traffic and filtering packets as needed |
| Wireshark | Network protocol analyzer; records and examines network packets, decrypts protocols | Transform network traffic into playable video for in-depth analysis |

According to (Bella et al. 2023) the table presents a foundational toolkit employed by researchers to explore vulnerabilities within the Tapo C200 IoT camera. This toolkit comprises essential software utilities, including Ettercap for executing Man-in-the-Middle attacks, Nessus for conducting comprehensive vulnerability scans, Nmap for swift network reconnaissance, SSL Packet Capture for decrypting encrypted data streams, Iptables for administering firewall configurations, and Wireshark for meticulous analysis of network packet traffic. In relation to IoT device vulnerability, the presence of such tools emphasizes the potential security risks associated with IoT cameras like the Tapo C200. Weaknesses in encryption protocols, such as those used for Wi-Fi communication, can be exploited by attackers using tools like SSL Packet Capture to intercept and decrypt sensitive data, compromising user privacy and security. A hidden but deadly threat, eavesdropping entails surreptitiously listening in on conversations in order to obtain private information. According to (Rachakonda, Siddula, and Sathya 2024) because the spectrum is shared, IoT devices that utilize it for spectrum sharing, especially within the framework of 5G networks, are particularly vulnerable to this danger. There is an increased risk of eavesdropping because 5G spectrum allocation is dynamic and densely packed, which makes it possible for unauthorized parties to intercept sensitive data transmitted by Internet of Things (IoT) devices that use mobile signal technology to exploit flaws in shared spectrum access.

**Vulnerabilities in Bluetooth Versions**

It is crucial to consider the Bluetooth version in use as well as the security of inter-device communications, which is dependent on the device with the oldest and weakest version. The vulnerabilities found in previous versions of Bluetooth persist because many older devices are still in use today. According to (Barua et al., 2022) list five main

Bluetooth versions were released by Bluetooth SIG on table 4. Every version is compatible with the others. Here are some key elements of each edition that are covered.

**Table 4**: Five main Bluetooth versions vulnerabilities

| Bluetooth Version | Release Year | Transfer Speed | Notable Features | Risks/Vulnerabilities |
|---|---|---|---|---|
| Bluetooth 1.0 and above | 1998 | Up to 1 Mbit/s | Initial release | - Security issues in pairing process<br>- Limited speed limit |
| Bluetooth 2.0 and above | 2005 | Up to 3 Mbit/s | Simplified pairing process | - Security issues in pairing process |
| Bluetooth 3.0 and above | 2009 | Up to 24 Mbit/s | Higher data transfer speed | - Higher power consumption |
| Bluetooth 4.0 and above | 2010 | Varies | Low Energy (LE) feature, IPv6 support | - Potential vulnerabilities in Low Energy (LE) feature.<br>-Security concerns with indirect IoT device connection |
| Bluetooth 5.0 and above | 2016 | Varies | Significant performance improvement | - Potential vulnerabilities in enhanced features and higher data transfer |

**Table 5** : Various tools commonly on Bluetooth security research and exploitation

| Tool | Function |
|---|---|
| CYW920819EVB-02 |  |
| BBC Mircobits V2 |  |
| Semiconductors nRF52840 |  |
| Flipper zero |  |

The Table 5 outlines various tools commonly employed in Bluetooth by previous security research and exploitation activity. According to findings by (Cook et al. 2024), the tool for Bluetooth analysis, it was observed that the BBC Microbit V2 demonstrates better performance compared to the Semiconductors nRF52840 BLE. These tools are used

for a variety of tasks, including managing and configuring Bluetooth devices, fraud hyperlink key authentication purposes, downgrading encryption keys, setup the human-computer interaction user interface, scanning and enumerating Bluetooth gadgets, and patching firmware in real-time.

The hacking attempts use the same tool, according to (Arreaga et al. 2023), perform sniffing on Internet of Things devices. Wireshark and the Ettercap program were also used to view the victim's password and login information.

**Table 6 :** Comparison of WiFi and Bluetooth Vulnerability Assessment Steps with Flipper Zero

| Step | WiFi Vulnerability Assessment | Description | Bluetooth Vulnerability Assessment | Description |
|---|---|---|---|---|
| 1. | Power On Flipper Zero: Ensure it's functional. | Ensure Flipper Zero is powered on and working properly. | Device Inventory: Create a detailed list of Bluetooth devices. | Create a comprehensive inventory of Bluetooth devices in scope. |
| 2. | Access Wi-Fi Signal Capture: Navigate to capture feature. | Access Flipper Zero's menu to initiate Wi-Fi signal capture mode. | Bluetooth Scanning: Use Flipper Zero to scan for nearby devices. | Use Flipper Zero to scan for nearby Bluetooth devices, noting their addresses and names. |
| 3. | Configure Capture Settings: Set channel, security, etc. | Configure Wi-Fi capture settings including channel and security. | Device Profiling: Gather device information including version and services. | Gather information about Bluetooth devices including version, supported profiles, and services. |
| 4. | Start Wi-Fi Capture: Initiate signal capture. | Begin capturing Wi-Fi signals based on configured settings. | Vulnerability Scanning: Use Flipper Zero for vulnerability assessment. | Utilize Flipper Zero to scan for known vulnerabilities, outdated firmware, etc. |
| 5. | Monitor and Record: View and store captured data. | Monitor Wi-Fi capture process in real-time and store captured data. | Pairing & Authentication Assessment: Evaluate security of pairing methods. | Evaluate security of Bluetooth pairing and authentication mechanisms. |
| 6. | Stop Wi-Fi Capture: End signal capture process. | Halt Wi-Fi capture process when desired data is obtained. | MITM Attacks: Test Bluetooth connections for susceptibility to MITM attacks. | Test Bluetooth connections for vulnerability to Man-in-the-Middle attacks. |
| 7. | Save Captured Data: Store data on SD card or computer. | Save captured Wi-Fi signal data for further analysis. | Replay Attacks: Assess resistance to replay attacks. | Assess Bluetooth devices' resistance to replay attacks. |
| 8. | Data Analysis: Analyze captured data using software tools. | Transfer captured Wi-Fi signal data to computer for analysis. | Sniffing Bluetooth Communication: Use Flipper Zero for communication analysis. | Use Flipper Zero to sniff Bluetooth communication and a |

According to (Winston James 2023) Flipper Zero is an electronic device that is capable of analyzing Table 6 and do vulnerability assessments for both Bluetooth and Wi-Fi. This device Flipper Zero is an open-source device with adaptable hardware that may be used to evaluate IoT devices for ethical hacking and pen testing. PENTOS is a specialist in IoT home device penetration testing, with a particular also on Bluetooth and WiFi technologies. According to (Yaacoub et al. 2023) it can test wireless communication protocols, online interfaces, and password security for vulnerabilities. After the evaluations, PENTOS offers a thorough analysis of assault outcomes that are unique to Bluetooth and WiFi in addition to customized security suggestions to improve the general security of IoT household devices This study looked into efforts at cyberattacks in smart home settings. According (Bhardwaj et al. 2024) the structure of the CPU was found, firmware assaults were proven to obtain name and credentials from the Internet of Things (IoT) firmware image using reverse engineering, and DoS attacks were used to take down the device in a matter of minutes.

**Figure 2** : Researchers provide result shown the weakness of Bluetooth version 4.0 until 5.1 on Blacktooth Attack and MITM Attack.

| Manufacturer | Device Model | Operating System | Chip Model | Producer | Bluetooth Version | Blacktooth Attack | MITM Attack |
|---|---|---|---|---|---|---|---|
| Apple | iPhone 12 | iOS 15.4.1 | 339S00761 | USI | 5.0 | ✓ | ✓ |
| Apple | iPhone 12 | iOS 15.0.1 | 339S00761 | USI | 5.0 | ✓ | ✓ |
| Apple | iPad Air 3 | iPadOS 15.2 | 39S00551 | USI | 5.0 | ✓ | ✓ |
| Apple | Macbook Pro 2018 | macOS Monterey 12.3.1 | BCM4364B0 | Broadcom | 5.0 | ✓ | ✓ |
| Google | Pixel 5 | Android 12.0 | Snapdragon 765G | Qualcomm | 5.0 | ✓ | ✓ |
| HONOR | V30 Pro | Harmony 2.0.0 | Hi1103 | HiSilicon | 5.1 | ✓ | ✓ |
| HONOR | V20 | Harmony 2.0.0 | Hi1103 | HiSilicon | 5.0 | ✓ | ✓ |
| HONOR | V8 | EMUI 8.0.0 (Android 8.0) | Kirin 955 | HiSilicon | 4.2 | ✓ | ✓ |
| HUAWEI | Mate 30 | Harmony 2.0.0 | Hi1103 | HiSilicon | 5.1 | ✓ | ✓ |
| HUAWEI | Mate 9 | EMUI 9.1.0 (Android 9.0) | BCM43455XKUBG | Broadcom | 4.2 | ✓ | ✓ |
| HUAWEI | P10 | EMUI 9.1.0 (Android 9.0) | BCM43455XKUBG | Broadcom | 4.2 | ✓ | ✓ |
| OnePlus | 9R | ColorOS 11.2 (Android 11.0) | Snapdragon 870 | Qualcomm | 5.1 | ✓ | ✓ |
| OnePlus | 7 Pro | Hydrogen OS 9.5.9 (Android 9.0) | WCN3998 | Qualcomm | 5.0 | ✓ | ✓ |
| OPPO | Find X2 Pro | ColorOS 12.1 (Android 12.0) | Snapdragon 865 | Qualcomm | 5.1 | ✓ | ✓ |
| OPPO | A72n 5G | ColorOS 7.2 (Android 10.0) | MT6853V | MediaTek | 5.1 | ✓ | ✓ |
| realme | X50 5G | realme UI 2.0 (Android 11.0) | WCN3998 | Qualcomm | 5.0 | ✓ | ✓ |
| Redmi | K30 Pro | MIUI 12.5.4 (Android 11.0) | WCN3998 | Qualcomm | 5.1 | ✓ | ✓ |
| Samsung | Galaxy S10 | One UI 3.1 (Android 11.0) | KM8D03042 | Murata | 5.0 | ✓ | ✓ |
| Xiaomi | Mi 10 Pro | MIUI 12.5.12 (Android 11.0) | QCA6391 | Qualcomm | 5.1 | ✓ | ✓ |
| Xiaomi | Mi 10 | MIUI 13.0.4 (Android 12.0) | QCA6391 | Qualcomm | 5.1 | ✓ | ✓ |
| Lenovo | ThinkPad X1 Carbon (5th) | Windows 10 Pro 1909 | 8265 | Intel | 4.1 | * | * |
| Lenovo | ThinkPad X1 Carbon (5th) | Linux 4.14.111 | 8265 | Intel | 4.1 | * | * |

✓ Confirmed to be vulnerable to the Blacktooth attack.
* Cannot complete a secure connection establishment after changing profiles

According to (Ai et al. 2022), from the Figure 2 researcher provide result shown the weakness of Bluetooth version 4.0 until 5.1 on Blacktooth and Man-In-The-Middle Attack. The table demonstrates that numerous devices with Bluetooth capability (4.1 to 5.1) have been shown to be exposed to the Blacktooth harm. This means that these devices have weaknesses in their Bluetooth implementation, firmware, or security features, making them susceptible to unauthorized access, data interception, or compromise by attackers. It's crucial for users of these devices to apply security updates promptly to reduce the risk of exploitation. Additionally, some devices encountered difficulties in completing a secure connection establishment after changing profiles, highlighting the need for thorough security testing and remediation efforts by manufacturers.

## 4. Future Hacking Trend

### New risk on IOT device base on wireless vulnerability

As IoT home devices equipped with Machine Learning (ML) and Artificial Intelligence (AI) capabilities become more prevalent, they present both new opportunities and challenges for cybersecurity. Furthermore, to improving technology functionality, these cutting-edge features might result in malicious parties looking to take advantage of these systems' complexity. The following are examples of possible wireless networking attacks against such devices.

- Adversarial Attacks on ML Models: These attacks aim to alter machine learning algorithms by introducing malicious data during training or taking advantage of weaknesses in the model, which might result in harmful or incorrect predictions.
- Data Interception and Manipulation: By intercepting wireless communications between the cloud and AI-enabled IoT devices, attackers may be able to introduce or modify fake data, affecting the device's ability to make decisions.
- Privacy Breaches: Malicious actors may take advantage of wireless connection vulnerabilities to obtain unauthorized access to private user information handled by AI algorithms, which could result in identity theft or other privacy violations.

- Denial-of-Service (DoS) Attacks: These involve flooding a wireless network with traffic or focusing on the communication channels of the AI-enabled device in order to interfere with its operation and cause a denial of service.
- Model Poisoning Attacks: These involve inserting poisoned samples into the AI model's training data in an effort to affect the model's behaviour in unanticipated ways.
- Anomaly detection evasion: AI-enabled Internet of Things devices frequently use anomaly detection as a security measure. In an attempt to avoid detection methods, hackers can try to alter the device's learning process.
- AI Decision-Making Exploitation: To obtain unauthorized access to systems or control linked devices within the Internet of Things ecosystem, attackers may attempt to take advantage of the conclusions made by AI algorithms.
- Firmware Exploitation: AI-enabled IoT devices may have their integrity compromised by firmware vulnerabilities that could lead to data theft or unauthorized control.

## 5. Discussion

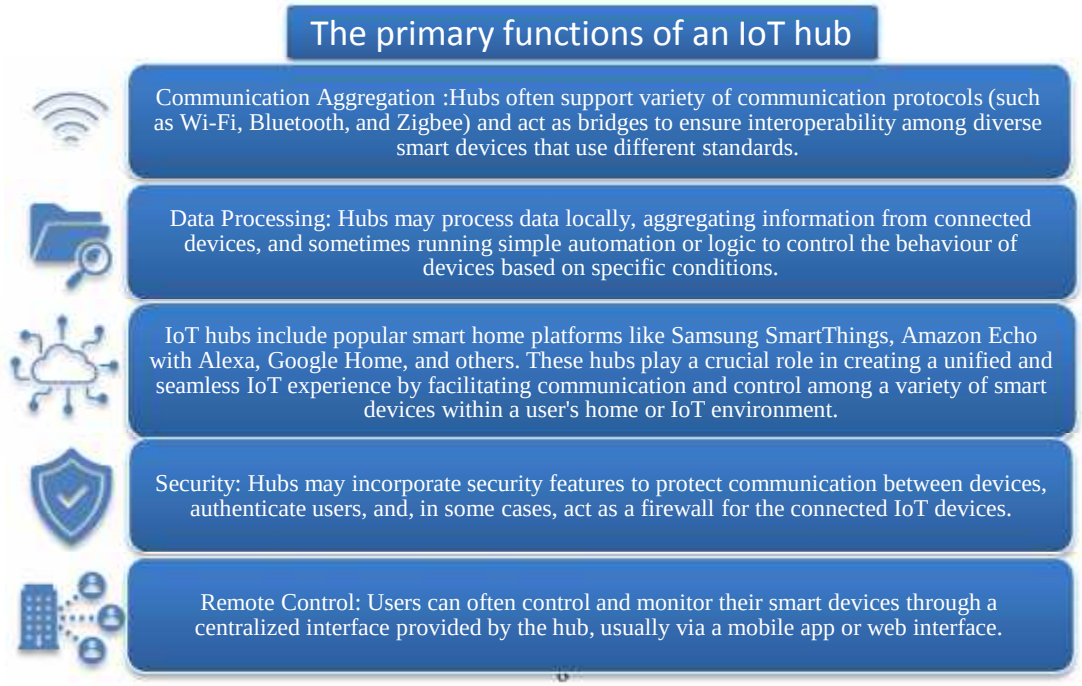
One category of IoT devices that hackers are likely to target due to security update vulnerabilities is legacy or outdated smart home hubs. These central devices often serve as the control centres for various interconnected smart devices within a home, managing communication and automation. As manufacturers release security updates to address vulnerabilities, legacy smart home hubs may become unsupported, leaving them susceptible to exploitation.

Hackers may specifically target these devices as they are less likely to receive timely security patches, making them an attractive entry point for unauthorized access to the entire smart home ecosystem. For instance, an older-generation smart home IoT device with outdated firmware might have unpatched vulnerabilities, allowing hackers to exploit weaknesses in communication protocols or gain unauthorized control over connected devices, compromising the security and privacy of the entire smart home network. This emphasizes the importance of regularly updating and replacing outdated IoT devices to ensure ongoing security.

### Internet of Things Hub

In the context of IoT (Internet of Things), a "hub" typically refers to a central device that serves as a communication gateway or control center for multiple connected devices within a smart home or IoT ecosystem. The hub acts as a central point for managing and coordinating the communication and interaction between various smart devices, such as sensors, actuators, and other IoT-enabled devices.

**Figure 3** : Primary functions of an IoT hub



## 6. Security Guidelines for IoT Device on Wireless Communication

To enhance the cybersecurity posture for consumers utilizing IoT devices at home, the following recommendations are made on below table.

**Table 7 :** Recommendations for Enhancing Security of IoT Home Devices

| Recommendation | Description |
|---|---|
| Firmware Updates and Patch Management | Regular updates and patches for IoT device firmware to fix known vulnerabilities and improve overall security. |
| User Authentication and Authorization | Enhance user authentication procedures and implement strong authorization systems to reduce unauthorized access to IoT devices. |
| Data Encryption Standards | Implement effective encryption standards for data transferred between devices and networks to prevent interception. |
| Vendor Accountability | Source IoT devices from reliable suppliers prioritizing security and evaluate vendor security procedures to reduce risks. |
| User Education and Awareness | Provide users with information about potential risks and recommended security practices to decrease the likelihood of cyberattacks. |

According to (Cäsar et al. 2022) in order fix known security problems in IoT products which are currently in use, patching or modifying the affected code is usually required. To avoid future security flaws, a device's capacity to update all of its software layers is essential, especially for those that are intended to be used for an extended period of time.This table provides a clear overview of each recommendation along with its description for enhancing cybersecurity in IoT device usage at home. According to (Shrestha et al. 2021) it's critical for users to recognize the warning indications of a possible piconet breach because of the simple it is to hack into one. Easy PINs and out-of-date Bluetooth security software on consumer devices are just two examples of the many vulnerabilities. According to (Md Zaglul Shahadat et al. 2023) since decrypting a WPA/WPA2 password takes longer than other password cracking techniques, it is preferable to regularly change the WiFi router's password at predetermined intervals to prevent unauthorized users or devices from connecting to the network. Additionally, by keeping an eye on the WiFi network, unexpected device or user access can be blocked and eliminated. To ensure that their products are secure for consumers to use, IoT device manufacturers must regularly assess the security of their products.

According to (Sarker, Yunus, and Deraman 2023) an organization must be aware of the vulnerabilities' priority, pertinent cost, complexity, and fixing time even if it chooses to forgo fixes on specific vulnerabilities to increase security. A penetration tester needs to use metrics to determine the importance of the vulnerabilities and remedial tasks. According to (Schiller et al. 2022) It will be necessary for consumers to exercise responsibility and security awareness, with the backing of laws, policies, and governments that sufficiently monitor this market. Customers should put security first and be mindful of any potential risks when using IoT devices.

## 5. Conclusion

In summary, the study offers insightful information about the state of security for popular communication protocols in the context of smart homes. The study focuses on important areas like authentication methods, encryption techniques, and general robustness as it methodically investigates the dangers and weaknesses related to Bluetooth and Wi-Fi-enabled Internet of Things devices. This research is important because it contributes to the growing topic about protecting residential IoT ecosystems, especially as smart devices increase across houses. The study provides information on potential risks and weaknesses, which in turn helps to build better security procedures, best practices,

and solutions. The results highlight the importance it is to solve security issues with Bluetooth and Wi-Fi enabled devices to protect the confidentiality, integrity, and robustness of smart home environments.

The study provides a first but important step in improving the security posture of residential IoT ecosystems, focusing future research attempts, and promoting the development of more secure IoT solutions as the IoT environment evolves. To create a safer and more secure IoT ecosystem for residential usage, manufacturers and users can benefit from the conclusions and recommendations made for preventing cyberattacks on IoT devices.

## 7. Acknowledgments

The authors would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia.

## References *:*

Ahmed Adbeib, Khaled. 2023. 2 African Journal of Advanced Pure and Applied Sciences *African Journal of Advanced Pure and Applied Sciences (AJAPAS) Comprehensive Study on Wi-Fi Security Protocols by Analyzing WEP, WPA, and WPA2*.

Ai, Mingrui, Kaiping Xue, Bo Luo, Lutong Chen, Nenghai Yu, Qibin Sun, and Feng Wu. 2022. "Blacktooth: Breaking through the Defense of Bluetooth in Silence." In *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, 55–68. doi:10.1145/3548606.3560668.

Ariyadi, Tamsir, and M. Rizky Pohan. 2023. "Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators." *Jurnal Penelitian Pendidikan IPA* 9(12): 10768–75. doi:10.29303/jppipa.v9i12.5551.

Arreaga, Nestor X., Genessis M. Enriquez, Sara Blanc, and Rebeca Estrada. 2023. "Security Vulnerability Analysis for IoT Devices Raspberry Pi Using PENTEST." In *Procedia Computer Science*, Elsevier B.V., 223–30. doi:10.1016/j.procs.2023.09.031.

Bella, Giampaolo, Pietro Biondi, Stefano Bognanni, and Sergio Esposito. 2023. "PETIoT: PEnetration Testing the Internet of Things." *Internet of Things (Netherlands)* 22. doi:10.1016/j.iot.2023.100707.

Bhardwaj, Akashdeep, Salil Bharany, Anas W. Abulfaraj, Ashraf Osman Ibrahim, and Wamda Nagmeldin. 2024. "Fortifying Home IoT Security: A Framework for Comprehensive Examination of Vulnerabilities and Intrusion Detection Strategies for Smart Cities." *Egyptian Informatics Journal* 25. doi:10.1016/j.eij.2024.100443.

Cäsar, Matthias, Tobias Pawelke, Jan Steffan, and Gabriel Terhorst. 2022. "A Survey on Bluetooth Low Energy Security and Privacy." *Computer Networks* 205. doi:10.1016/j.comnet.2021.108712.

Cook, Stephen, Royal Holloway, Maryam Merhnezad, Ehsan Toreini, and Maryam Mehrnezhad. 2024. "Bluetooth Vulnerabilities in General and Intimate Health IoT Devices and Apps: The Case of Female-Oriented Technologies." doi:10.21203/rs.3.rs-3877210/v1.

Fatima, Haram, Habib Ullah Khan, and Shahzad Akbar. 2021. "Home Automation and RFID-Based Internet of Things Security: Challenges and Issues." *Security and Communication Networks* 2021. doi:10.1155/2021/1723535.

Heiding, Fredrik, Emre Süren, Johannes Olegård, and Robert Lagerström. 2023. "Penetration Testing of Connected Households." *Computers and Security* 126. doi:10.1016/j.cose.2022.103067.

Md Zaglul Shahadat, Mhia, Matsive Ali, Avijit Mallik, and M Matsive Ali. 2023. *An Approach on Cracking WPA,WPA2 Security of Wi-Fi with Handshake Attack*. https://www.researchgate.net/publication/368241744.

Nor Naematul Saadah, Ismail, and Zolkipli Mohamad Fadli. 2023. 184 International Journal of Computer Applications *Preliminary Review of Phishing Attacks and Countermeasures on the Internet of Things (IoT) Environment.*

Rachakonda, Lakshmi Priya, Madhuri Siddula, and Vanlin Sathya. 2024. "A Comprehensive Study on IoT Privacy and Security Challenges with Focus on Spectrum Sharing in Next-Generation Networks(5G/6G/Beyond)." *High-Confidence Computing*: 100220. doi:10.1016/j.hcc.2024.100220.

Rudrakar, Santoshi, and Parag Rughani. 2023. "IoT Based Agriculture (Ag-IoT): A Detailed Study on Architecture, Security and Forensics." *Information Processing in Agriculture*. doi:10.1016/j.inpa.2023.09.002.

Sadikin, Fal, Nuruddin Wiranda, Jl Brigjen, Jalan Hasan Basri, Kec Banjarmasin Utara, Kota Banjarmasin, and Kalimantan Selatan. 2023. *Sadikin and Wiranda-Investigation and Penetration of Digital Attacks on Zigbee-Based IOT Systems INVESTIGATION AND PENETRATION OF DIGITAL ATTACKS ON ZIGBEE-BASED IOT SYSTEMS*.

Sarker, Kamal Uddin, Farizah Yunus, and Aziz Deraman. 2023. "Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods." *Sustainability (Switzerland)* 15(13). doi:10.3390/su151310471.

Schiller, Eryk, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, and Burkhard Stiller. 2022. "Landscape of IoT Security." *Computer Science Review* 44. doi:10.1016/j.cosrev.2022.100467.

Shrestha, Sunny, Esa Irby, Raghav Thapa, and Sanchari Das. 2021. *SoK: A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures*. doi:http://dx.doi.org/10.2139/ssrn.3959316.

Winston James, DrJoy. 2023. *Evaluating IoT Device Security: Penetration Testing and Vulnerability Assessment with Flipper Zero*. https://ssrn.com/abstract=4658141.

Yaacoub, Jean Paul A., Hassan N. Noura, Ola Salman, and Ali Chehab. 2023. "Ethical Hacking for IoT: Security Issues, Challenges, Solutions and Recommendations." *Internet of Things and Cyber-Physical Systems* 3: 280–308. doi:10.1016/j.iotcps.2023.04.002.