e-ISSN: 2349-2678, p-ISSN:2961-6050

available online on www.ijpba.in

International Journal of Pharmaceutical and Biological Science Archive

NLM (National Library of Medicine ID: 101732687)

Index Copernicus Value 2022: 72.59

Volume 12 Issue 1; 2024; Page No. 21-28

CYBER SECURITY CHALLENGES WITHIN THE CONNECTED HOME ECOSYSTEM FUTURES

P. Vivekanand[1], Dr. Kusum Rajawat [2]

[1]Research Scholar, Sunrise University, Alwar
[2]Associate Professor, Sunrise University, Alwar

Article Info: Received: 12-10-2023 / Revised: 20-11-2023 / Accepted: 10-12-2023
Address for Correspondence: P. Vivekanand
Conflict of interest statement: No conflict of interest

Abstract

The future of linked home ecosystems is far closer to cybercrime and cyber security risks than was previously believed. Most studies examine the protection mechanisms of government and corporate networks, but the gadgets utilized in today's and tomorrow's linked smart homes provide a significant vulnerability. This report is a component of a larger study looking at the effects and obstacles posed by cybersecurity threats to internet-connected smart gadgets in the home. We discuss the history and drivers behind the increasing need for all of our smart gadgets to work together seamlessly, so that we can provide our consumers access to a wide range of features and capabilities. Despite these technologies' increased utility, the report stresses the fact that they also pose new dangers. Then, we go into the current cybersecurity concerns surrounding smart devices in smart homes and examine them in depth.

Keywords: cyber security, cybercrime, cyber physical systems, connected home, mobile malware.

Introduction

New process breakthroughs in businesses are being driven by the IoT's network of connected equipment and gadgets that are capable of two-way communication and collaboration. Cybersecurity assaults on Internet of Things (IoT) systems have become more common and widespread, causing several problems for individuals and businesses in the areas of credibility, regulation compliance, financial stability, and daily operations. The spectacular proliferation of IoT devices in fields including smart grids, environmental monitoring, patient monitoring systems, smart manufacturing, and logistics has contributed to the alarming rise in cyberattacks. The dynamic and transitory nature of the connection between devices, the variety of actors capable of engaging inside IoT systems, and resource limits all contribute to making IoT security management difficult.

The increased amount of cyberattacks on IoT devices, expanding IoT security laws, and growing security concerns are all factors that are predicted to drive the global IoT security market to develop at a CAGR of 33.7% between 2018 and 2023. Senior management will need to pay greater attention to IoT-related risks when implementing organization-level cyber risk management, according to a new poll. This is because IoT-based threats will grow more ubiquitous and impactful. However, just 35% of respondents say they have an IoT security plan in place, and only 28% of those say they've really put it into action. According to yet another poll, 80 percent of businesses have had cyberattacks on their IoT devices during the previous 12 months. However, the report indicates that 26% of the businesses surveyed did not use any kind of security technology. These two studies highlight the necessity for proactive investment in IoT cybersecurity by businesses and highlight the security gaps in many IoT devices.

Existing risk assessment methodologies are not suited to dynamic systems like the IoT, despite the fact that security measures are inadequate. For instance, the intricacy of medical IoT systems leaves them vulnerable to a variety of attacks, but current risk assessment approaches aren't well suited to evaluating this kind of threat. To avoid unintentionally increasing cyber threats, businesses may benefit from developing IoT systems on a uniform platform.

The goal of Internet of Things cybersecurity is to safeguard IoT assets and user data in order to lessen the impact of cyberattacks on businesses and individuals. IoT cybersecurity management faces both possibilities and problems presented by the ongoing development of new cybersecurity technology. The majority of existing research has focused on the technology elements of IoT security. The complicated cybersecurity risks in IoT systems, however, are seldom addressed due to the absence of comprehensive risk management frameworks. This study offers a literature analysis on IoT security technologies and cyber risk management frameworks and builds a four-layer IoT cyber risk management framework in light of the current deficiency in IoT cybersecurity risk management. The article then presents a linear programming approach to deciding how best to fund various initiatives aimed at securing the Internet of Things. The risk assessment is finally shown using an example of IoT cyber risk management for a hotel smart room.

LITERATURE REVIEW

Rashmi Anand (2018) The SAPLAP models in this case study are built using both systematic inquiry and matrices. The actors who are responsible for and involved in IT policy making, infrastructure building, and the execution of e-Government are categorized. Synthesis of SAP components led to additional case study learning through synthesis of diverse LAP parts. The influence of the effectiveness, i.e. the transformation of information security, policy, and e-Governance, on the Digital India plan has been stated, along with a summary of the key activities and performance. After constructing the SAP-LAP framework, it became clear that some players, such as India's Ministry of Electronics and Information Technology, are in a better position to push forward the goal of e-Government by enacting different initiatives and central sector plans. More investments in IT infrastructure, policy creation, and a method to manage cyber security concerns are examples of the actions of other desirable players that would facilitate the efficient implementation of e-Governance. It was determined that players should take the initiative to improve technical skills, capacity development, and the dissemination of knowledge about ICT-related governmental applications and e-Governance. To better handle transition, policymaking, and the government process in India's administration, as well as to help the country's economy reach the Sustainable Development Goals, policymakers can look to the sustainable management practices of e-Governance project execution as a guide.

William C. Banks (2017) This case study uses both in-depth research and SAPLAP models built on matrices. Classification of actors responsible for and involved in IT policy formulation, infrastructure development, and e-Government deployment. The case study's lessons were built around a synthesis of SAP components and subsequent synthesis of LAP parts. Appropriate measures and results have also been underlined, and the results of the transformation of information security, policy, and e-Government on the Digital India project have been stated. The SAP-LAP framework's development revealed that key players, such as India's Ministry of Electronics and Information Technology, rank highly in putting into action a number of initiatives and central sector plans designed to speed up the country's e-Government agenda. For e-Government to be successfully implemented, other desirable actors' actions, such as increased investments in IT infrastructure, policy creation, and a framework to manage cyber security concerns, are necessary. It was determined that stakeholders should take the initiative to improve their knowledge of ICT applications and e-Governance via training and education.

When it comes to the management of change, policy making, and the government process in the Indian administration, as well as the attainment of Sustainable Development Goals by the Indian economy, decisions should be founded on the sustainable management practices of implementation of e-Governance projects.

Aabid Rashid Wani, (2022) One of the most promising innovations right now is the Heterogeneous Network (HetNet) that incorporates Unmanned Aerial Vehicles (UAVs). This technology is useful for meeting the extensive bandwidth, data volume, and transmission distance requirements of various users. In this research, the authors implement Identity based Scheme (IBA), an authentication-based security protocol, to guarantee the safety of the network's users. Network data privacy and user verification are both bolstered by IBA-based solutions. The entity's ability to verify, sign, and trade authenticated data without central directory involvement contributes to privacy and dependability. Since HetNets supported by UAVs are particularly vulnerable to intrusion, the major goal of this study is to develop an identity-based authentication system for use in such networks. Security is bolstered and the risk of catastrophic intrusion is reduced as a result. The implementation zones in this study are intended to serve as defensive watchtowers from which the adversary may be located or as other strategic elements. Security policies are written in a programming language called High Level Protocol Specification Language (HLPSL), and AVISPA is used to validate the final products.

ChunHua Cao, (2021) Issues with wireless sensor networks (WSN) include low resources, inadequate computer power, ineffective communication, and susceptibility to assault. However, when applied to WSN, the current encryption algorithms cannot adequately resolve the aforementioned issues. To this aim, an enhanced identity-based encryption algorithm (IIBE) is presented that may efficiently streamline the key generation process, lessen the load on the network, and tighten up security for WSNs by building on the foundation of identity-based encryption. This technique takes a middle ground between classic public key encryption and identity-based public tweezers' encryption in terms of its conceptual architecture. The approach removes the hassle of maintaining a public key certificate, which is required by conventional public key encryption methods. The technique solves the issues of key escrow and key revocation, which plague identity-based public key encryption. Experimental findings from a real-world network reveal IIBE's low power consumption and good security, making it an ideal candidate for use in WSNs where privacy and data integrity are of the utmost importance.

METHODOLOGY

Security Threats on Smart Devices

Users are the weakest link in any information technology security system. The biggest obstacle to mobile device security is the people using them. Most people who use electronic gadgets at home trust the manufacturer's default settings rather than reading through lengthy user guides. This means that the people who provide the devices and the services we use every day need to know what is expected of them in terms of network security and content management. To compensate for the devices' flaws, service providers may be able to provide supplementary security services. Cybersecurity is a far more domestic concern. Therefore, the cybersecurity issue is not limited to desktop computers; it also poses a risk to mobile gadgets. From cell phones to game consoles to automobile navigation systems, many common household electronics are essentially minicomputers. These gadgets increase convenience and efficiency but can present new dangers. These advances in technology may allow attackers to breach previously protected equipment. According to the POSTnote on cyber security in the UK, the information stored and handled on such devices and home networks constitutes individuals' Critical Information Infrastructure (CII) .

Your smart gadget might be infected with malware, your mobile phone or wireless service could be stolen, and your tablet's data could be hacked. These actions may have major ramifications for your privacy if you save sensitive personal or company data on your smart device. Seventy-six percent of smartphone users, according to a survey by Juniper Networks use their phones to access highly confidential data including financial and health records. Those who use their own mobile devices for work will see this tendency even more so. Almost nine out of 10 (89%) business users say they have accessed confidential company data using their mobile device. The possibility of hackers to use the network's massive resources to transform it into a botnet and launch a cyber-attack on national vital infrastructures is another, more frightening aspect. An unprecedented 155 percent surge in mobile malware assaults was recorded in 2011 across all platforms, according to research from Juniper Networks' Mobile Threat Centre (MTC) .

TVs, digital picture frames, smart meters, and e-readers are just a few examples of potentially susceptible and capable gadgets that might cause issues on your network. Malware creators of all stripes will have the next several years to experiment with outlandish strategies for attaining their nefarious ends. Malware, such as CVE-2012-0507, is also a problem for Macs and there are vulnerabilities in smartphones. A flaw in the Samsung D6000 high definition (HD) TV was discovered by Luigi Auriemma in, which allowed the TV to restart indefinitely. After Gabriel Menezes Nunes discovered a denial-of-service (DoS) vulnerability in Sony Bravia TVs, which prevents users from adjusting the volume, changing channels, or accessing any features, Auriemma reported on it. As the number of people using and exposing Android-based devices to cyber threats increased, the number of assaults on such devices increased as well.

This vulnerability is being targeted by well-known hacker organizations like Anonymous, and it will pose a greater danger to smart settings that secure highly sensitive data by allowing hackers to zero in on specific persons for political or financial gain. Wireless communications allow phishing not just through e-mail, as is the case with PCs, but also via SMS and multimedia messaging services (MMS), making mobile phishing especially popular among hackers. According to Trend Micro's first quarterly report of 2012, the widespread availability of mobile devices and the spread of knowledge about the most significant cyber dangers have piqued the criminal community's interest in the mobile industry.

Threat Assessments

Because the availability and usage of smart linked devices is expected to rapidly rise in the future, we give a description of some of the security dangers related to the future connected home. The major security issues, it is assumed, lie in the corporation, while consumers' loyalties lie at home. The house is quickly becoming a front in the war for consumer electronics supremacy. Every day, we have more and more tools at our disposal in the domestic sphere. This poses a major vulnerability in the devices' ability to communicate and stay secure. Equally important is the seamless interoperability of these gadgets, which will allow us to receive previously unimaginable levels of service. It is also crucial to provide home users an easy-to-use interface for setting and modifying the system's security settings.

It is probable that sensors/devices linked to the network, or the servers that receive, store, and analyze information from the sensors, will be the target of security threats and attacks on connected home infrastructures. Both types of susceptibility must be taken into account. They are the system's weakest link because of the device or sensors attached to fake gadgets. Everything from basic temperature monitors to elaborate video surveillance systems for everything from private residences and public streets to oil pipelines in distant locations may be linked to the Internet. Figure 1 illustrates how cyberespionage naturally follows the trend of 2013's most common data breach vector: online apps. Targeting smart gadgets or insecure home networks is significantly simpler for these attackers. Most online purchases are made over private home networks and smart devices, and a recent survey found that almost half of web application cyber-attacks target shops. One difficulty is the low cost of basic devices or sensor devices; for widespread adoption, it will be necessary to build in security to the networks of devices from the outset, rather than attempting to add it after the fact.

While cyber-security professionals have made strides in protecting servers and networks from assaults over the last several decades, the rise of the Internet of Things (IoT) and smart homes has prompted them to reevaluate their strategies. Isolating protective control systems from other networks was an important tactic. With the widespread Internet connectivity of today's control systems, the strategy is no longer viable. In light of this, a user-centric security system with several layers is essential, one that provides stronger access controls, content management, and network monitoring in addition to protecting individual devices, servers, networks, and applications.

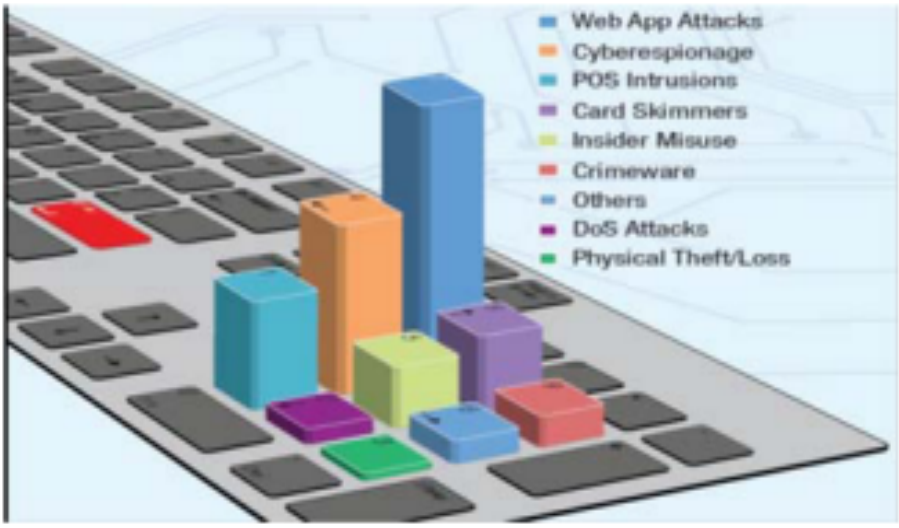


Figure 1: Data Breaches 2013

Innovations in the Internet of Things and the smart home have opened up promising new avenues, but only if they can be relied upon to perform as promised. The moment to begin addressing these issues is now. Half of all mobile apps send either location data or personal information to the cloud , thus scam apps and social engineering are only going to become more of a problem.

x Lost Or Stolen Devices

The rising mobility of today's workforce increases the likelihood that important company tools may be misplaced or stolen. About 10% (18.5 million) of the 187 million compromised identities discovered by Symantec in 2011 were due to a lost device.

x Open Wi-Fi And Public Network

Consumers (and by extension, workers) are sloppy with mobile phone security, according to studies. Wi-Fi assaults are on the increase, according to a new analysis from Juniper Networks, since unsecured networks provide cybercriminals easy access to users' personal information via email and social media. Unfortunately, many people are still unaware of the dangers of using public Wi-Fi networks, especially ones that seem to be "closed."

x Malware And Viruses

New technologies herald the arrival of spyware with new capabilities. Malware has two primary varieties . First, government, law enforcement, or private companies may use agents-based systems to create and run surveillance on targeted users, networks, or services. Second, it was created and is controlled by a criminal ring or groups of criminals that seek to profit from the widespread use of malware. A recent Symantec analysis reveals that risks to smartphone security are on the rise. One group allegedly made $1 million employing this method every year, as detailed in a study by Symantec. It is not necessary for the crooks to have access to a large number of phones.

X Corporate Policy

While the rising consumerization of IT and the advantages it brings to employees may not appear like a security risk at first glance, the lack of defined corporate rules to manage new technology poses a real risk. When it comes to the gadgets and productivity apps accessible to employees, many companies are overwhelmingly supportive of employee choice. However, these same businesses have been hesitant to implement regulations to safeguard against the risks posed by new technology. The majority (57%) of respondents believed that attacks originated from inside the company, followed by customers (10%).

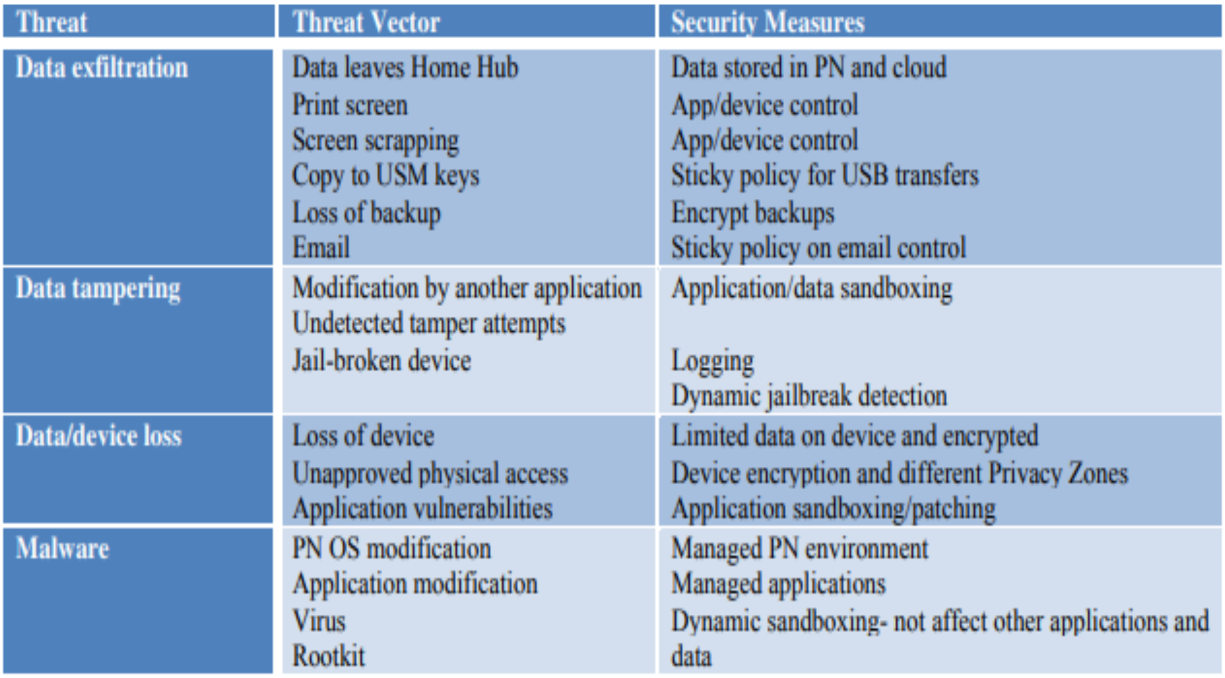
X Theft/Abuse of Services

The ecosystem of a smart home has both internal and external service providers and consumers. These services must benefit the user or some aspect of the network in order to be considered valuable. The advantage from these services might be taken by an attacker. Smartphone malware that taps into the user's mobile broadband connection without permission and then bills them for the data use is an example of service theft. An attacker stealing this service could use a victim's device to do computational activities, including cryptocurrency mining, which is considered an internal service.

X Unauthorized Cyber-Physical Control

Recently, hackers have considered using cyber-physical systems to achieve their goals. Any computing system that is embedded in the network and may exert influence on external physical infrastructure is considered cyber-physical in the context of the ecosystems of the linked homes of the future. It's probable that this will also support access from afar. Some examples of cyber-physical systems include (future) smart meters and household products that can manage the physical environment, such as smart refrigerators, lighting controls, and HVAC systems. A primary goal of cyber-physical systems is to give the user more agency over their immediate surroundings, and these systems often provide this capability through the user's private network. Consequently, an unlawful takeover of cyber-physical infrastructure might be the end goal of an assault on the individual's network. This attack goal is unlikely to be a major issue in the future of the linked home ecosystem at this time, but it is likely to become so as the number of smart cyber-physical devices grows. A starting point for future and existing efforts to improve the security of personal networks is the quick description of some of the dangers described above. Table 1 summarizes some of the prevention strategies we propose for the identified dangers.

Table 1: Threats and counter measures



Threat	Threat Vector	Security Measures
Data exfiltration	Data leaves Home Hub Print screen Screen scrapping Copy to USM keys Loss of backup Email	Data stored in PN and cloud App/device control App/device control Sticky policy for USB transfers Encrypt backups Sticky policy on email control
Data tampering	Modification by another application Undetected tamper attempts Jail-broken device	Application/data sandboxing Logging Dynamic jailbreak detection
Data/device loss	Loss of device Unapproved physical access Application vulnerabilities	Limited data on device and encrypted Device encryption and different Privacy Zones Application sandboxing/patching
Malware	PN OS modification Application modification Virus Rootkit	Managed PN environment Managed applications Dynamic sandboxing- not affect other applications and data

CONCLUSIONS

The research examined the potential dangers that hackers may face in the future from exploiting vulnerabilities in connected home ecosystems. Experts in cyber security predict that in the near future, home infrastructures will be the primary target of hackers and the greatest difficulty for them to handle. As the number of people using mobile smart devices grows tremendously, so too will the number of malicious programs and the sophistication of the assaults they launch. This is especially true for the Android platform. Users nowadays often do private and sensitive tasks, such as online banking and payments, using their mobile smart devices. Users' increasing reliance on mobile devices as digital wallets is a tremendous problem for security professionals and a potentially profitable target for hackers. Users of mobile banking and other financial services may anticipate a surge in malicious software. Our previous publications have proposed frameworks and provided some implementations to deal with some of the identified threats discussed in this paper, and this work is part of ongoing research to design and implement a security model for smart devices in smart home connected ecosystem futures. Our future work will center on creating a sandbox where cybersecurity professionals may experiment with new approaches to the ever-evolving problem of protecting critical infrastructure from cyberattack.

REFERENCES

1. Anand, R et al. (2018), ―Transforming Information Security Governance in India (A SAP-LAP based case study of security, IT policy and egovernance)‖, Information & Computer Security, (26) 1: 58-90.
2. Banks, W. C. (2017), ―Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage‖, Emory Law Journal, Vol. 66, 513-525.
3. Wani, A.R.; Gupta, S.K.; Khanam, Z.; Rashid, M.; Alshamrani, S.S.; Baz, M. A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. IET Intell. Transp. Syst. Early View 2022, 1–19.
4. Cao, C.; Tang, Y.; Huang, D.; Gan, W.; Zhang, C. IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. Secur. Commun. Netw. 2021, 2021, 1–8.
5. Cao, C.; Tang, Y.; Huang, D.; Gan, W.; Zhang, C. IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. Secur. Commun. Netw. 2021, 2021, 1–8.
6. Zhang, L.; Ma, M.; Qiu, Y. An enhanced handover authentication solution for 6LoWPAN networks. Comput. Secur. 2021, 109, 102373.
7. Mbarek, B.; Ge, M.; Pitner, T. Proactive trust classification for detection of replication attacks in 6LoWPAN-based IoT. Internet Things 2021, 16, 100442.
8. Ingham, M.; Marchang, J.; Bhowmik, D. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. IET Inf. Secur. 2020, 14, 368–379.
9. Ugwuanyi, S.; Paul, G.; Irvine, J. Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics 2021, 10, 2224.
10. Kuntke, F.; Romanenko, V.; Linsner, S.; Steinbrink, E.; Reuter, C. LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios. Trans. Emerg. Telecommun. Technol. 2022, 5, 33.
11. Seoane, V.; Garcia-Rubio, C.; Almenares, F.; Campo, C. Performance evaluation of CoAP and MQTT with security support for IoT environments. Comput. Netw. 2021, 197, 108338. Bilal, D.; Rehman, A.U.; Ali, R. Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP. Int. J. Comput. Appl. 2018, 179, 9–14.
12. Tsai, W.C.; Tsai, T.H.; Wang, T.J.; Chiang, M.L. Automatic Key Update Mechanism for Lightweight M2M Communication and Enhancement of IoT Security: A Case Study of CoAP Using Libcoap Library. Sensors 2022, 22, 340.
13. Park, J.H.; Kim, H.S.; Kim, W.T. DM-MQTT: An Efficient MQTT Based on SDN Multicast for Massive IoT Communications. Sensors 2018, 18, 3071.

14. Lee, J.G.; Lee, S.J.; Kim, Y.W. Attack Detection and Classification Method Using PCA and LightGBM in MQTT-based IoT Environment. J. Inf. Secur. 2022, 22, 17–24.
15. Hussein, N.; Nhlabatsi, A. Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control. IoT 2022, 3, 450–472.