IoT Performance and Security Analysis Based on WiFi Systems

Michael Raj Mosas[1](✉), Azwan Mahmud[1], Noorlindawaty Binti Md Jizat[1], Azlan Abd. Aziz[2], and Syamsuri Yaacob[3]

[1] Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia
[2] Faculty of Engineering and Technology, Multimedia University, Melaka, Malaysia
[3] Faculty of Engineering, Universiti Putra Malaysia (UPM), 43400 Serdang, Selangor, Malaysia

Abstract. With the introduction of the Internet of things (IoT), the number of wireless devices and volume of wireless data traffic has skyrocketed. The system proposed in this paper focuses on Internet of things (IoT) performance and security analysis based on Wi-Fi systems. In order to perform this analysis, an IoT wireless temperature and humidity sensor will be developed; whereby, the microcontroller will communicate and send collected data to an IoT cloud platform where the collected data can be analyzed and stored. An android application is developed from scratch to fetch the data from the IoT cloud platform, display the data in the application and send messages to the cloud. The sensor, microcontroller and the android application will communicate wirelessly with each other through Wi-Fi and MQTT (MQ Telemetry Transport) protocol. The performance and security of the whole system will be tested and analyzed; and ways to improve both the performance and security of the IoT system is presented. The system is subjected to Distributed Denial-of-Service (DDoS) attack, with Security Information and Event management (SIEM) is implemented for detection and DDoS attack prevention.

Keywords: Cybersecurity · IoT Platform · Risk assessment

1 Introduction

Internet of things, or IoT, is a network of interconnected computing devices, electronics devices such as sensors, microcontroller, software and other technologies that can connect and exchange data with other devices and systems over the Internet or other communications networks. Because of the integration of numerous technologies, such as ubiquitous computing, commodity sensors, increasingly sophisticated embedded systems, and machine learning, the IoT research area has progressed rapidly [1–8].

IoT is a new paradigm that has shifted people's lifestyles from conventional to high-tech. IoT is widely applied in many fields from commercial, industrial and infrastructure spaces. Wi-Fi is one most used communication medium in IoT environment. IoT have been growing fast in the last several years and this leads to several risk especially in the areas related to security and privacy of data and system [9, 20].

The main problem arises when a IoT environment involves important and private data which must be protected from outsider, and common IoT attacks in order to maintain

© The Author(s) 2023
M. Y. bin Alias (Ed.): MECON 2022, AER 214, pp. 3–13, 2023.
https://doi.org/10.2991/978-94-6463-082-4_2

the privacy and integrity of the IoT environment. This is required in order to maintain a secured IoT environment and to achieves the full potential of IoT and enhance technology through Internet of Things [7]. By 2023, the number of IoT-connected devices in the world is expected to reach 43 billion. According to surveys 84 percent of companies use IoT devices on their corporate networks, and more than half of them don't use security measures other than default passwords [20].

IoT connections are frequently used by cybercriminals to infiltrate network infrastructure and steal personal information. Threat actors use unpatched vulnerabilities and manufacturing flaws in connected devices to gain access to corporate networks. IoT are still vulnerable to multiple cybersecurity attacks such as DDOS Attack, Brute force attack and Privilege Escalation Attack [7–10]. IoT devices are not designed to detect or mitigate any potential cyberthreat. Unless they are not protected, serious risk could pose to organizations. In order to understand and prevent these cyberthreats various research must be done to improve the security and performance of IoT networks [6, 20].

Following are the remaining parts of this article. The related work is discussed in Sect. 2. While in Sect. 3, we have the Methodology and then the Simulation and Results from this study was place in Sect. 4. And lastly, we have our conclusions in Sect. 5.

2 Related Works

The authors of [1] discusses the features of IEEE802.11n/ac (Wi-Fi) and how it performs in dense IoT environments. The studies were mainly focus on the influence of the density and type of IoT traffic on the wireless system's throughput, bandwidth consumption of RTS and CTS frames, block acknowledgments, and frame aggregation sizes was examined using a real test bed consisting of large number Raspberry Pi's installed in a real-world setting.

Challenges regarding cyber threat and risk assessment for IoT environment based on Wi-Fi are highlighted in [20]. This paper provided a detailed study on security of the Wi-Fi IoT environment and stated analysis on three important vulnerability such as Device Port Weak Management Vulnerability in where they talk about the vulnerabilities of the communication ports of the IOT devices.

In addition to above mentioned risk and threats, the energy efficiency of constrained device using Wi-Fi were focused in [3]. The main solidity of this research is its low-cost build and using three different types of batteries mainly used in most IoT and daily electronic devices in order to test it energy efficiency which gave more options and ways to look into Wi-Fi's energy efficiency in depth. Multiple Wi-Fi authentication policies were used to measure the power consumption by measuring the duration of each wakeup period and also by varying the Sleep Period the battery consumption have been directly influenced with different duty cycles.

The authors of [2] present a wireless system and to develop an alert system in order to monitor the readings of the wireless system which mainly focuses on embedded device and the IoT network rather than Wi-Fi.

With the evolution in Cloud services integration in IoT, traditional SIEM paradigm is shifting to provide Cloud based security services. The authors of [6] presented an upgraded upgraded SIEM architecture composed of a SIEM Framework to provide

Cloud based SIEM service. A solution for end-to-end IoT Platforms security using cybersecurity framework and its three components Cybersecurity risk assessment, SIEM, and resilience frameworks were provided.

Similarly, in [4] a framework for detecting API unauthorized access vulnerabilities was proposed. The framework was implemented to analyse the problem of API unauthorized access vulnerability in the android platform. The paper highlighted the impact of API unauthorized access vulnerabilities on various smart home application and devices and also provided some defensive suggestions on how to prevent it effectively. It was very effective on performing check on the cloud platform for API's security problems.

In order to perform the security and performance analysis on a IoT system based on Wi-Fi, in our work, a model consists of an ESP8266 and DHT11 module for transmitting temperature and humidity data via MQTT protocol [2, 3]. An MQTT brokers are used to receive and store the data values along with an Android application to communicate with the MQTT broker via MQTT protocol and having two main functions which is publishing and subscribing to the MQTT broker [15–18]. DDOS attacks will be simulated on the system and tools such as Wireshark will be used to monitor the network and the MQTT packets. In order offer a solution against the DDOS attack, an SIEM software will be used to provide security [13, 14].

Our such, our contribution in this paper is as follows:

- Our end to end IoT setup is based on MQTT connection that is able to connect to any MQTT brokers (Adafruit, Amazon Web Services (AWS), Thingspeak etc.) as long as the correct key and username being applied while existing literature connected to a single broker.
- Simple and low cost for end to end IoT system using WiFi, Cloud and MQTT broker. The setup is using simulated DDOS traffic test, it can be easily extended for future research on mitigating and preventing other types of cybersecurity attacks on IoT networks.

3 Methodology

A. Design Overview

Figure 1 shows the IoT model working together with SIEM [14] in order to mitigate and prevent DDOS attacks against the model [6, 7]. In this work, in order to perform the security and performance analysis on a IoT system based on Wi-Fi a wireless IoT Temperature and Humidity system using ESP8266 and DHT11 sensor [2, 19] will be created and transmits data to the cloud.

An Android application will be created to communicate to the cloud. The communication between the IoT system [2], Cloud and application will be using MQTT protocol to test the security and performance of the whole system. Instead of using HTTPS or API method, MQTT protocol will be used to enhance the performance of the system and provide a secured connectivity between the cloud, android application and the IoT system. The mobile application will be built from scratch and will be fully functional [12, 15–19].

Additionally, A DDOS attack will be simulated to attack the IoT system and the application. performance and security deterioration of the system will be analyzed. A

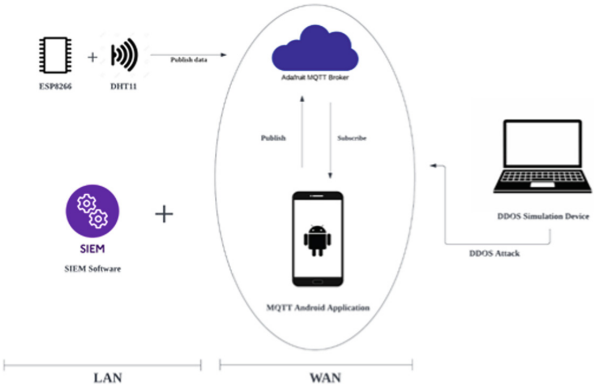

Fig. 1. IoT Model

third-party software will be used to stimulate the DDOS attack from a different IP addresses [7]. Moreover, SIEM will be implemented to mitigate the DDOS attack and introduce to methods to prevent DDOS attack to restore the security and performance of the IoT system and the application. The Round-Trip-Time of the TCP packets will be measured along with the ping to determine the delay cause by DDOS attack and how the SIEM and the prevention technique helps stop the DDOS attack [6, 7].

B. Android application

The android application was built from scratch using Android studio and based on Kotlin language (Fig. 2).

The android application has two main pages which are the Login page and Publish/Subscribe page. This application was designed to communicate with MQTT broker to publish message and also to subscribe to a topic to receive message. The unique feature of this application is that it can connect to any MQTT broker as long username and password is provided to login and establish a connection to the MQTT broker [2, 15–18].

This feature allows a greater potential for the application enabling it to connect to any MQTT broker. Once logged on, the user can publish message to the MQTT broker and communicate with it. A pop-up message will be displayed when there is successful or unsuccessful connection have been made to the MQTT broker. The user can also subscribe to a topic through the MQTT broker and receive message. We tested with AWS, Thingspeak, Adafruit and some other MQTT servers. For example, our android application will be subscribing to the Adafruit.io and display the temperature and humidity values through a pop message in the interval of every 60 s [2, 15–18].

Even though the application is fully functional and can be installed in a mobile phone it will be operate in device using the android virtual devices (AVD) manager with the built Android emulator in Android studio in order to simulate DDOS attack on the selected device and the packets can be sniffed using Wireshark at the same time along with the Cloud running on the same device [7, 12].

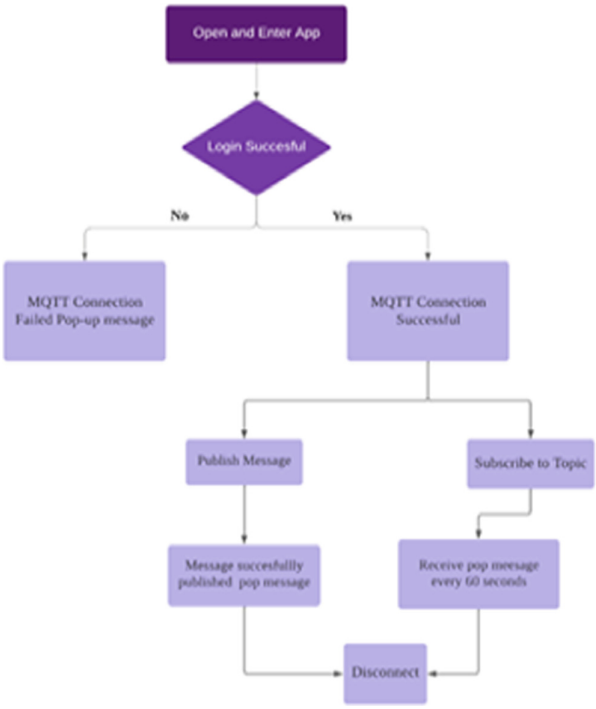

Fig. 2. Application Flowchart

C. SIEM and DDOS Prevention Methods

SIEM starts monitoring and collecting information of the entire system. After configuring the SIEM can start viewing the syslog. Syslog is a standard network-based logging protocol that logs every activity in the network. SIEM takes advantage of the syslog to monitor and collect information [12–14]. When there is DDOS attack, with the aid of syslog SIEM starts tracking the flooding of UDP or ICMP packets [11] to the network and it also able to collect information about the details of the DDOS Attack source such as the IP address [7, 10]. With its built-in framework the SIEM is able to differentiate and recognize the malicious attack on the network thus allowing the user to detect the DDOS attack before it interrupts the whole systems services. It alerts the user immediately when it starts detecting the DDOS attack on the network [6, 14].

Figure 3 shows the flowchart of SIEM and how it is used to stop or prevent DDOS Attack against the network [6, 8]. Once the SIEM detect anomalies in the network and it alerts the user. Slow network is resulted from DDOS Attack on the network and by checking the syslog, the flood of UDP and ICMP packets on the network can be confirmed [11]. This shows that the network is under DDOS attack. Immediate actions have to be taken in order to stop this DDOS attack. Firstly, SIEM identifies or collect information about the source of DDOS attack [8, 12–14]. Once the IP of the DDOS Attack source have been obtained that particular IP can be blocked thus stopping all the Packets flood from the network and DDOS attack or by changing the IP of the device under DDOS

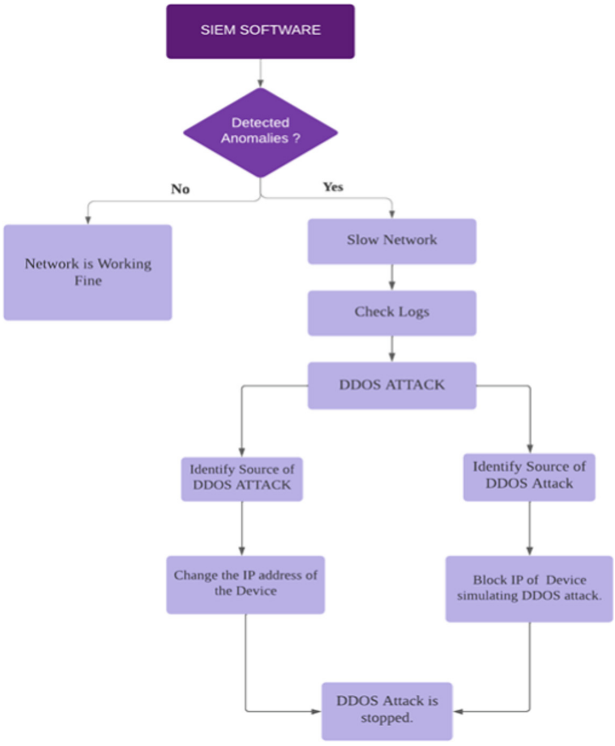

Fig. 3. Using SIEM to Prevent DDOS Attack

attack, the flood of packets can be stopped because it is IP targeted DDOS attack. In order for the DDOS attack to happen, it needs a fixed IP or the sources IP address [11] must be unknown if have two of these variables changes the DDOS attack can be solved effectively [12–14].

4 Result and Discussion

In this section, the round-trip-time of the MQTT packets and ICMP packets sniffed by Wireshark before and after DDOS attack will be discussed. ICMP packets were used while determining the ping of network. The results obtained after using the SIEM and DDoS prevention methods will be determined. One of the important measurement is the transmission of successful data in the IoT network, and the security and performance of the network before and after DDOS attack.

Figure 4 shows the round-trip-time of the MQTT packet before the DDOS attack have been executed. The round-trip time of 6 MQTT packets averages by 41.67 ms while Fig. 5 shows round-trip time of the MQTT packets after DDOS attack has been executed. This is a UDP based DDOS attack; this type of DDOS attack floods a target with large number of UDP and TCP packets which aims to flood random host port on a

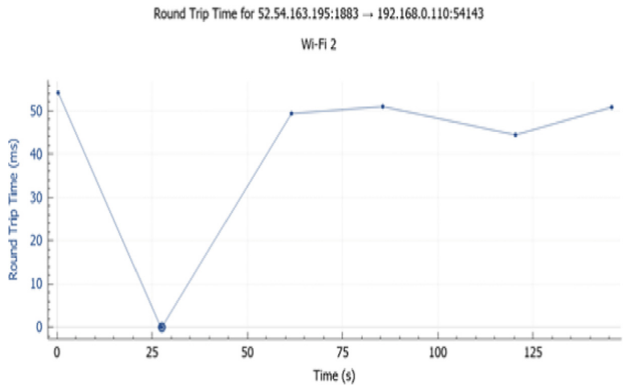

Fig. 4. RTT of MQTT Packet before DDOS Attack

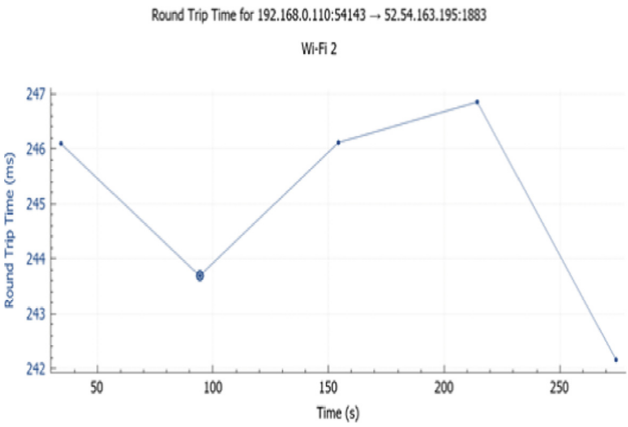

Fig. 5. RTT of MQTT Packet After DDOS Attack

remote host resulting in causing the host to repeatedly check for application to listen to that port. The round-trip time of 5 MQTT packets averages by 244.92 ms.

By comparing the Fig. 4 and 5, it shows a big difference of almost 200 ms increase in the round-trip time of the MQTT packets. A clear indicator of DDOS attack increases the latency of a network and disrupt the normal service. These increase in RTT can cause a slow network and makes the MQTT packets to longer time to response thus affecting the overall performance of the IoT network, any maybe can cause a timeout of the web services.

Figure 6 shows the ping statistics for the Adafruit MQTT broker before the DDOS attack. The average round-trip-time of the ICMP packets which are used to test ping of a network is 361 ms. The Fig. 7 shows the ping statistics for the Adafruit MQTT broker after the DDOS attack. This is an ICMP based DDOS attack. It sends ICMP packets as fast as possible without waiting for replies causing the other ICMP replies to be delayed and increase the round-tip time. By comparing Fig. 6 and 7, there is a significant difference

```
PING 52.54.110.50 (52.54.110.50) 56(84) bytes of data.
64 bytes from 52.54.110.50: icmp_seq=1 ttl=63 time=0.361 ms
64 bytes from 52.54.110.50: icmp_seq=2 ttl=63 time=0.412 ms
64 bytes from 52.54.110.50: icmp_seq=3 ttl=63 time=0.413 ms

--- 52.54.110.50 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.361/0.395/0.413/0.024 ms
```

Fig. 6. Network Ping (Adafruit) before DDOS

```
PING 52.54.163.195 (52.54.163.195) 56(84) bytes of data.
64 bytes from 52.54.163.195: icmp_seq=1 ttl=63 time=0.620 ms
64 bytes from 52.54.163.195: icmp_seq=2 ttl=63 time=0.595 ms
64 bytes from 52.54.163.195: icmp_seq=3 ttl=63 time=0.553 ms

--- 52.54.163.195 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.553/0.589/0.620/0.027 ms
```

Fig. 7. Network Ping (Adafruit) after DDOS

in the average round-trip time which is about 192 ms. An increased ping causes a delay in response from the server which disrupt all the activities in the network thus slowing down the connection in the IoT network.

We then introduced SIEM in the network. Once there is a DDOS Attack on the network, the SIEM automatically detects the attacks and alerts the user for prevention. The attacks are then prevented in a way, by changing the IP address of the device under DDOS attack or blocking the IP address of the source of DDOS attack. Figure 8 and 9 shows, the RTT and ping of the network after SIEM identifies the source of DDOS attacks and the IP of DDoS attacking source have been blocked or the IP address of the device under attack is changed. The RTT of the MQTT packets averages by 49.083 ms and the ICMP packets averages by 373 ms.

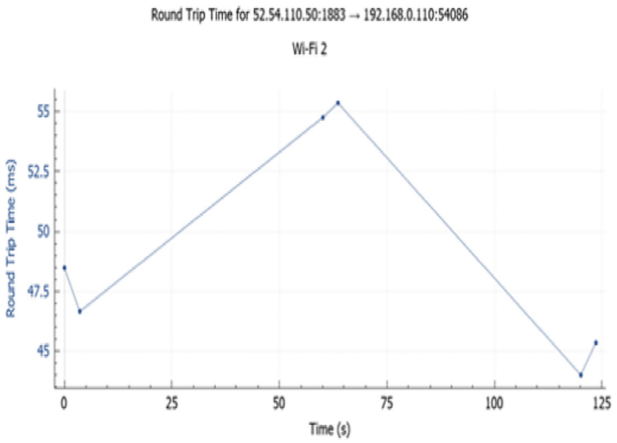

Fig. 8. RTT after SIEM implementation and DDOS Attack Prevention Method

```
PING 52.54.110.50 (52.54.110.50) 56(84) bytes of data.
64 bytes from 52.54.110.50: icmp_seq=1 ttl=63 time=0.373 ms
64 bytes from 52.54.110.50: icmp_seq=2 ttl=63 time=0.441 ms
64 bytes from 52.54.110.50: icmp_seq=3 ttl=63 time=0.419 ms

--- 52.54.110.50 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2040ms
rtt min/avg/max/mdev = 0.373/0.411/0.441/0.028 ms
```

Fig. 9. Network Ping after SIEM implementation and DDOS Attack Prevention Method

5 Conclusion

In this study, we proposed a system to prevent and stop DDoS attack on IoT network. The main results that were focused were the round-trip time of the MQTT and ICMP packets before and after the simulation of DDOS attack and the implementation of SIEM to detect the DDOS attack and way to prevent the attack. It also shows its performance and security effect on the IoT network. These data can be used to improve an IoT network's security and performance against cybersecurity attacks.

Acknowledgments. The work is supported by FRGS/1/2020/TK02/ MMU/03/1(MMUE/190229) grant and RIPHEN ENERGY4.0: HVAC conservation through chiller optimization and control with IoT.

References

1. Ganji, G. Page and M. Shahzad, "Characterizing the Performance of WiFi in Dense IoT Deployments," 2019 28th International Conference on Computer Communication and Networks (ICCCN), 2019, pp. 1-9.
2. M. F. A. Samsudin, R. Mohamad, S. I. Suliman, N. M. Anas and H. Mohamad, "Implementation of wireless temperature and humidity monitoring on an embedded device," 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2018, pp. 90-95.
3. F. Montori, R. Contigiani and L. Bedogni, "Is WiFi suitable for energy efficient IoT deployments? A performance study," 2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI), 2017, pp. 1-5.
4. Y. Li, Y. Yang, X. Yu, T. Yang, L. Dong and W. Wang, "IoT-APIScanner: Detecting API Unauthorized Access Vulnerabilities of IoT Platform," 2020 29th International Conference on Computer Communications and Networks (ICCCN), 2020, pp. 1-5.
5. Y. Zhang, Y. Lin, Z. Dou, M. Wang and W. Li, "Monitoring and Identification of WiFi Devices for Internet of Things Security," 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1-5.
6. S. K. Datta, "DRAFT - A Cybersecurity Framework for IoT Platforms," 2020 Zooming Innovation in Consumer Technologies Conference (ZINC), 2020, pp. 77-81.
7. G. Yadav, A. Allakany, V. Kumar, K. Paul and K. Okamura, "Penetration Testing Framework for IoT," 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), 2019.
8. K. Sornalakshmi, "Detection of DoS attack and zero-day threat with SIEM," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), 2017, pp. 1-7.
9. Internet of things and big data analytics toward next-generation intelligence. Nilanjan Dey, Aboul Ella Hassanien, Chintan Bhatt, Amira Ashour, Suresh Chandra Satapathy. Cham, Switzerland, 2018.
10. "What is a DDoS Attack? - DDoS Meaning". usa.kaspersky.com, 2021-01-13. 52
11. "Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4". Cisco, 2019-08-26.
12. J. Lee, Y. S. Kim, J. H. Kim and I. K. Kim, "Toward the SIEM architecture for cloud-based security services," 2017 IEEE Conference on Communications and Network Security (CNS), 2017.
13. M. Hristov, M. Nenova, G. Iliev and D. Avresky, "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT," 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA), 2021, pp. 1-5
14. F. Holik, J. Horalek, S. Neradova, S. Zitta and O. Marik, "The deployment of Security Information and Event Management in cloud infrastructure," 2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA), 2015, pp. 399-404
15. W. -T. Su, W. -C. Chen and C. -C. Chen, "An Extensible and Transparent Thing-to-Thing Security Enhancement for MQTT Protocol in IoT Environment," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-4
16. Amelia et al., "MQTT Protocol Implementation for Monitoring of Environmental Based on IoT," 2020 International Conference on Applied Science and Technology (iCAST), 2020, pp. 700-703
17. Team, The HiveMQ. "Introducing the MQTT Protocol - MQTT Essentials: Part 1". www.hivemq.com, 2021-09-26.
18. "Client, Broker/Server and Connection Establishment - MQTT Essentials: Part 3". www.hivemq.com, 13 October 2019.

19. R. K. Kodali and K. S. Mahesh, “A low cost implementation of MQTT using ESP8266,” 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016, pp. 404-408
20. Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), “IoT Device (Wi-Fi) Security Study” March 2020, pp. 1-17.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.