A SECURITY ANALYSIS ON MQTT PROTOCOL OF IoT

BY

LOKNATH DHAR SAGAR
ID: 171-15-9204

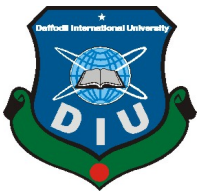
This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

MS. REFATH ARA HOSSAIN
Lecturer
Department of CSE
Daffodil International University

Co-Supervised By

Mr. GAZI ZAHIRUL ISLAM
Assistant Professor
Department of CSE
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2022

APPROVAL

This Project/internship titled "**A Security Analysis on MQTT Protocol of IoT**,", submitted by Loknath Dhar Sagar, ID No: 171-15-9204 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 04 January, 2022.

BOARD OF EXAMINERS

Chairman

Dr. S.M Aminul Haque (SMAH)
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Raja Tariqul Hasan Tusher (THT)
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Md. Sazzadur Ahamed (SZ)
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology

External Examiner

Dr. Shamim H Ripon
Professor
Department of Computer Science and Engineering
East West University

DECLARATION

I hereby declare that this project has been done by me under the supervision of **Ms. Refath Ara Hossain, Lecturer, Department of CSE** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

Ms. Refath Ara Hossain
Lecturer
Department of CSE
Daffodil International University

Submitted by:

Loknath Dhar Sagar
ID: 171-15-9204
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I express our heartiest thanks and gratefulness to Almighty God for His divine blessing makes it possible to complete the final year project successfully.

I am grateful and wish my profound indebtedness to **Ms. Refath Ara Hossain**, **Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "**Network Security**" to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting them at all stages have made it possible to complete this project.

I would like to express our heartiest gratitude to **Dr. Touhid Bhuiyan**, Professor and Head**,** Department of CSE, also to other faculty members and the staff of the CSE department of Daffodil International University.

I would like to thank my entire coursemate in Daffodil International University, who took part in this discussion while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

ABSTRACT

The Internet of things is currently a buzzword in the modern technology era. Over the years, the Internet of Things has become a part of our lives. For their integral behavior, many companies and solutions are built upon it. Though many solutions have been developed to meet the needs, security issues are still overlooked. MQTT is one of the most used protocols in the IoT world because of its performance, battery-friendliness. However, as many companies use this protocol to make their products, security is one of the significant issues of this protocol. In this report, we will take a look at the security issues of the MQTT protocol and analyze them for future researchers and studies. We will discuss some common vulnerabilities that are still not fixed or up to the developers' choice to implement security solutions that have been overlooked over the years. We will also discuss how researchers should approach the IoT security issues and provide a methodology for interacting with modern-day IoT protocols.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Introduction

In the era of technology, communication technology has brought us the possibility that we could not imagine a long time ago. In communication technology, the invention of ARPANET (which turned into the internet later) and the rise of the Internet of Things (IoT) brought special significance to the world. For example, the students of Carnegie Mellon University found a way to monitor the number of cans on a vending machine by using devices that can communicate with the internet. It was the very first implementation of the Internet of Things.

Though at first, the concept of IoT may look somewhat bizarre. Kevin Aston, who first used the term “Internet of Things,” would probably not have imagined that these devices would spread vastly worldwide. However, the internet of things has come a long way, improving from time to time. Nowadays, we can see this technology everywhere from household appliances to enterprises, retail stores, health care, industry, power grids, and scientific research.

The first pace of the rise of IoT devices created a dangerous situation where the policymakers could not develop quality and security controls. As a result, the world of IoT technology is continuously getting news of the security vulnerabilities of IoT devices. These incidents got the attention of the researchers, and they are working for better security for IoT devices as the IoT devices have already claimed their places in our daily lives.

1.2 Motivation

As IoT devices work by collecting the data and receiving it from the environment, exchanging it with other devices and systems over the internet, privacy and security are some of the main concerns in this field. According to a study by Transforma Insights, "7.6 billion IoT devices were already active at the end of 2019" [1], and it is expected that "it will grow to 24.1 billion by 2030" [1]. However, with the growth of IoT devices and systems, these continuously suffer from privacy and security issues. For example, hard-coded passwords, not changing the default password, lack of firmware updates have increased security risks and vulnerabilities and the chances of acquiring sensitive data. In addition, researchers consider IoT the most vulnerable technology for cyber attacks due to weak manufacturing, weak security protocols, hardware limitations, computational and energy constraints, memory constraints, and tamper-resistant packaging. As IoT began to explode in 2011, many security countermeasures and mechanisms were developed over the years; but security in IoT is still a problem these days.

From OWASP's top 10 list [2], it can be noticed that many vulnerabilities still exist in IoT technology. For example, weak, guessable passwords, insecure network services, insecure ecosystem interfaces are vulnerable to others, and the strength of the communication services between them.

If we look at the history of the IoT world, we can find many security issues happening from time to time. Hernandez et al. [3] mention security shortcomings from Google Nest, which allowed the attackers to install new malicious firmware on the device. It was found in 2013 that Philips hue and many other devices suffered security issues for identifying the MAC address of the host. The Lifx smart bulb used the 6LoWPAN protocol, which was vulnerable to malicious packets into the network. Jay Radcliffe [4] from Rapid7 identified that some medical devices like insulin pumps suffered from replay-based vulnerability. So the analysis is intended to focus on the security of protocol so that the future of the IoT remains secure and the practice of security analysis built up over the years.

1.3 Rationale of the study

The continuous rise of the Internet of Things led to the development of multiple protocols in the communications area. Each of them is attempting to meet the expectations of different uses to fulfill specific domains and problems. Sometimes these protocols share some vulnerabilities of the same type. As the internet of things is relatively young, these protocols are evolving, and new protocols are emerging to fulfill the environment's needs. Some protocols can also be designed to maintain the security standards securely, and others can create more security issues.

The primary purpose of this research is to highlight the current security issues in existing IoT protocols. Some well-known IoT protocols are AMQP, NB-IoT, CoAP, 6LowPAN, IPv6, Wi-Fi, Bluetooth, SigFox, ZigBee, Z-Wave. Security researchers have studied these protocols to develop better security and privacy over the years.

This report will focus on the current state of the protocols in terms of security and privacy, specifically on MQTT. In addition, we will also talk about some attack vectors of the IoT.

1.4 Expected Output

Our work is based on analyzing the protocol's network traffic structure. Also, on what other researchers have been found over the years, and the solutions of the vulnerabilities they suggested.

We expect to present the current state of MQTT and the existing security issues of some well-known protocols, which will help new researchers to conduct their research.

1.5 Report Layout

This report is divided into several sections.

- Chapter 2 will discuss the background of IoT security and related works
- Chapter 3 will discuss the research methodologies
- Chapter 4 will create a discussion and present the state of the IoT security research.
- Chapter 5 will discuss the current issues and future scope for the researchers.
- Chapter 6 will present the summary and conclusion.

CHAPTER 2
BACKGROUNDS

2.1 Terminologies

Internet of Things (IoT) is currently a buzzword for the modern world, a revolution in technology. The Internet of things is a collection of various network-enabled devices that can communicate, share information, and work together for decision-making; thus, they build a network. IoT consists of four basic building blocks - sensors, processors, gateways, and applications [5].

Sensors: Sensors are the front end of IoT devices. These are the "things" of the system. Their functions are to collect data from the environment or give out data to their surroundings. They have uniquely identifiable IP addresses and are active on their own or user-controlled.

DOI**cessors:** Processors are the brain of the system. Their functions are to process the data they gathered and make decisions depending on the information on a real-time basis.

Gateways: Gateways route the processed data and connect it to network devices, making the interconnected network send the data to the proper location.

Applications: Applications utilizes the data collected from the environment. They determine the final goals and outcomes of the system.

Applications send gathered data through gateways with the help of communication protocols. There are many communication protocols, but some are domain-specific, some for efficiency, and some are generic. Furthermore, all protocols have different implementation flaws, protocol design, and configuration. Examples are MQTT, AMQP, WebSocket, DNP3, DNS, BLE, RFID, ZigBee, etc.

2.2 Concepts of IoT

Security is a general and sensitive issue in this virtualization era because no rule ensures that a system is fully protected. Because the security characteristics can be tackled on so many levels and are subject to constant evolution technology [6]. Also, IoT security is different from traditional security because an IoT ecosystem is composed of embedded systems, sensors, mobile applications, clouds, and network communication protocols. Based on the IoT ecosystem, it can be divided into three categories:

1) Embedded Device;
2) Firmware, Software, and Applications;
3) Communications.

These introduced us to different attack surfaces on IoT.

2.2.1 Embedded Devices

An embedded device is the foundation of IoT architecture and the “thing” in the Internet of Things. So it will hold sensitive information, and if it is compromised, it would be considered critical. Serial ports exposing, power analysis, and side channel-based attacks, dumping the firmware over JTAG or via Flash chips or insecure authentication mechanism can be considered highly vulnerable.

2.2.2 Firmware, Software, and Application

A Hack study by Miller and Valasek [7] has shown that security concerns were not built for IoT. Authentication of the firmware which runs on its chips can be found, and the IoT world neglected it. It was not considered a security vulnerability initially. Authentication and authorization are IoT’s core concepts, and host-based secure booting will always ensure that authorized code can run on the IoT node [8].

As the whole firmware includes everything that runs on the device, these device interfaces are vulnerable to some extent. Web-based dashboard, insecure network interfaces are exposed over the network as they collect data and frequently end it to a distant point. It is the ideal attack surface. Some vulnerable surfaces are storage, authentication, and authorization of the devices, sensor, and peripheral interfaces. Some examples like modifying firmware, insecure signature, private certificates, outdated components with known vulnerabilities, side-channel data leakage, logic flaws, cross-site scripting are known in the security issues of the IoT world.

2.2.3 Communications

Commercial products are usually not considered protocols when it comes to the point of security. However, communication protocols like Wi-Fi, BLE, ZigBee, ZWave, 6LoWPAN, LoRA are used in IoT communications. As it is not usually considered about the protocol's security, IoT communication protocols are now the primary attack vector of the IoT world. Denial of Service (DoS) attacks, lack of encryption, jamming-based attacks, replay-based attacks are now prevalent in IoT communication security.

2.2.4 Attack Vectors

As the IoT ecosystem consists of embedded devices, software, and communication, we can divide the attack surfaces into three to four categories.

1. **Device:** The first one is the device itself. A device consists of storage which includes SD cards, USB, Volatile and non-volatile memory. This storage can be used to store firmware updates. Vulnerabilities can come from memory, firmware, physical interfaces, and network services. Unsecure default settings, firmware update mechanisms, and outdated components also attack IoT vectors.
2. **Cloud:** IoT is not only about hardware. It can also communicate with the internet, and the cloud plays a vital role in this area. Data can be held in the cloud, and it has the privileges to send and receive commands to them. If the cloud can be

compromised, which is deployed worldwide, attackers will gain access to the devices and the hazardous data [9]. It makes the cloud an interesting attack vector of the IoT world. From the study of Payatu, a cybersecurity service provider for IoT, they provide some attack vectors for the cloud such as authentication, encryption, APIs, etc.

3. **Communication:** The communication interfaces and the drivers/firmware are responsible for the transmission, but it falls under the device category. Hardware interfaces provide the actual communication, but the layers and protocols define the data [9]. A list of communication protocols can be used in the IoT ecosystem, where developers often overlook security solutions. A flaw in the protocol may result in attacks that also affect the endpoints such as devices or the cloud [9]. Payatu shows that authentication, encryption, and poor implementation of the protocol standard are the primary attack vectors for the communication. This report will discuss one of the most used IoT protocols, MQTT.
4. **Applications and Software:** Software related to the IoT ecosystem and web applications are also the attack vectors for IoT. By exploiting them, attackers can access the credentials, push malicious firmware updates and gain control of the IoT ecosystem.

Payatu [10] also published a list of top ten vulnerabilities for the IoT, which includes:

1. Hardcoded Sensitive information;
2. Enabled hardware debug ports;
3. Insecure Firmware;
4. Insecure data storage;
5. Insufficient Authentication;
6. Insecure Communication;
7. Insecure Configuration;
8. Insufficient data input filtration;
9. Insecure Mobile Interface;
10. Insecure Cloud/Web interface [10].

2.4 Comparative Analysis and Summary

Many researchers are currently working on IoT Architectures, Protocols, and Applications. As IoT is one of the most rising technologies, researchers are publishing analysis results and helping new researchers to work further. For example, Lombardi et al. [11] discussed top architectures, protocols, and applications of IoT. Their studies discussed the architecture layer of IoT and the most used protocols on the layer. Based on their research, CoAP, MQTT, DDS, AMQP, XMPP are the most used protocols on the application layer, TCP and UDP on the transport layer, LoWPANs, ZigBee, Z-wave, LoraWLAN, Sigfox, NB-oT on the Network layer.

Mohanty et al. [12] and his team presented a model for IoT security and privacy based on blockchain technology. They proposed the ELIB model based on blockchain and discussed the security features combining all the aspects of IoT. Cerney et al. [13] surveyed the application layer protocols' identification, authorization, and authentication. Yang et al. [14] summarised different security issues of IoT applications. Also, Tschofenig et al. [15] performed a study on the internet protocols suite for IoT security.

Shipley et al. [16] and Jing et al. [17] discussed various stages of the life cycle of an IoT attack and the IoT Security Requirements in their studies. Their list of IoT Security Requirements is Cryptographic Algorithms, Key Management Techniques, Secured Routing Algorithms, Data Classification, Protecting devices at production time, Secured Operating System, Application Security, Encryption, Network Connectivity, Secured Event Logging, etc.

Cynthia et al. [18] and her co-authors mentioned some security issues of IoT in their studies like Low power embedded devices, trust management, Secured Access Control, Identity Management, Trust Management, and Distributed IoT networks. In addition, their studies discussed some security challenges like dynamic security patches and limitations on network connections for mobility and scalability [18].

According to Liu et al. [19] and his co-authors, essential measures should be taken with different IoT protocols to communicate with various devices. Furthermore, the difference between protocols stops service contracts from implementation and are fundamental elements that should be present in the security structure of IoT architecture [19].

2.4 Scope of the Problem

Recently there has been an increase in the targeting of the communication protocols of IoT. Though vendors and developers are fixing many vulnerabilities, many exploitations are still not fixed. Researchers are working on different security aspects, discussing in-depth IoT technology, and proposing models and future factors. Our study will discuss the most used IoT protocol, MQTT, and its security designs and existing vulnerabilities. We will also discuss if vulnerabilities still exist and if new vulnerabilities are found or not. Our study focuses on the security aspects of the top Internet of Things protocols and helps developers and researchers to develop and improve the communication protocols. Covering all the exploits and vulnerabilities on all protocols can not be possible at the moment. This study will try to cover the most used communication protocols in IoT.

2.5 Challenges

As the growth of the internet of things increases day by day, new exploits and vulnerabilities are being found every day. Zero-day exploits and vulnerabilities (exploits that are not being reported by others) still exist at the time of this study. As these zero-day exploits are not reported, discussing them is not possible at the moment. Also, this study is trying to cover the existing vulnerabilities that developers should fix in terms of priority; covering all vulnerabilities is not the goal of this study.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Research Subject and Instrumentation

IoT Technologies differ from standard IT technologies. As IoT is being used in many areas, including medical spots, security failure can cause a direct loss of life. Implementation of proper security requires vast amounts of storage and computing power, which goes against the IoT concept, as a core concept of IoT is size and a power constraint. Also, unlike traditional security tests, IoT requires inspecting and working with new and different communication protocols which are not generally encountered in the general environment. In communication protocols and the device hardware, applications and interfaces need to be disassembled, analyzed, and studied as it is unique in terms of the internet of things.

Our studies will discuss MQTT, one of the most popular machine-to-machine communication protocols in the IoT world. It is being used in sensors, healthcare products, and small devices that require low power usage. It is based on a TCP/IP stack but extremely lightweight as it minimizes messaging using a publish-subscribe architecture.

MQTT stands for Message Queueing Telemetry Transport which is OASIS and ISO standard. Based on the principle of the Publisher-Subscriber mechanism, it is incredibly lightweight and works well in constrained and automated environments like machine-to-machine communication and IoT. Moreover, as it runs over TCP/IP stack, it can also run over other network protocols that provide reliable, bi-directional, and ordered communication.

There are some entities involved in the MQTT protocol. These are:

- **Publisher:** Publisher collects the data from sensors. It will publish data on a particular topic and transfer the information to subscribers via the broker.
- **Subscriber:** Subscriber subscribes to the topic on which publisher publishes data.
- **Broker:** Broker collects the data from the publisher and supplies it to the subscribers. The broker is a central device. The broker's responsibilities are processing the communication between clients and distributing the messages based on the clients'DOIpics. The broker can manage thousands of devices simultaneously [20]. When a broker receives a message on a particular topic, it searches all the devices subscribed to it and sends the data. In most scenarios, brokers store data in clouds, and the subscribers get via it, and processing the data becomes accessible.
- **Topic:** The address where the message is published is called topic.
- **Message:** Messages are the information.

MQTT is a very lightweight protocol by its generic design. As a result, it can provide low power consumption for devices and an ideal protocol for low-powered, smaller devices. Moreover, it is very battery friendly as studies found that it consumes less energy on 3G and Wi-Fi networks. So for the devices which need to stay connected for a long time, MQTT is an ideal protocol to use.

It also ensures 100% message delivery under poor network conditions. MQTT introduces three different flags known as Quality of Service (QoS).

- **QoS 0:** At most once delivery. This is the default level for MQTT, suitable for reliable network connections where data loss is acceptable. In addition, it provides the highest possible speed.
- **QoS 1:** At least once delivery. At this level, the broker sends the message and ensures that the message is received at least once. QoS 1 is used when the system needs the message delivery guarantee and allows duplicate messages.

- **QoS 2:** Exactly once delivery. This level is used in critical network conditions where the system needs the message delivery guarantee but does not allow duplicate messages. This level provides the highest messaging quality and is very reliable.

As MQTT is battery-friendly, lightweight, and ensures message delivery, this protocol is very well known to the IoT world. Moreover, the automotive industry is also considering using MQTT to build connected cars [21].

3.2 Proposed Methodology

3.2.1 Information Gathering

The act of gathering various kinds of information about a system is called information gathering. In the information-gathering phase, we will try to find resources available to us which we can use against a targeted system. In our case, searching the official and unofficial documentation about the targeted protocol falls under information gathering. Also, various resources like developer blogs and enthusiasts' blogs can be enormous resources for the targeted protocol.

3.2.2 Installing and Enumerating clients

To gather a specific understanding of the protocol, we have to create a test environment to check and analyze the protocol in life. To create an environment, we can gather clients which can communicate with the protocol. We can also generate and replicate network traffic to analyze them closely. Implementations in different programming languages can be another resource to understand the protocol better as other clients communicate with the protocol differently.

3.2.3 Discovering the different protocols

As the IoT world consists of different technologies, IoT protocols can sometimes depend on the other protocols. For example, the TCP/IP stack is the primary transport protocol in our interconnected world, and many protocols rely on the TCP/IP stack for communications. Therefore, to get a clear understanding of how secure a protocol is, we have to look for the dependencies of that protocol.

3.2.4 Protocol's Port and Certificate Authentication

Protocols run on different types of ports. To create tools to exploit the protocols, we have to find the default port number of that protocol. There are so many different protocols in our interconnected world, and some protocols run on alternate ports. Identifying them will be a significant step in analyzing IoT protocols.

3.3 Implementation Requirements

To create a test environment for our desired purpose, we will use Virtualbox with Kali Linux. We have to develop network traffic to communicate with the protocol to analyze specific protocols. Therefore, we are using well-known clients which can communicate with our desired protocol. In the case of MQTT, we will use Eclipse Mosquitto Software as it acts as a server and broker at the same time. In addition, we are using a famous, open-source network traffic capture tool Wireshark to capture and analyze network traffic.

CHAPTER 4
EXPERIMENTAL RESULTS

4.1 Experimental Setup

We will conduct our analysis in Kali Linux, a penetration distribution designed for pen-testers, security researchers, and students. We have already set up our Kali environment (Version 2021.2, released on 1st June 2021) in the Virtualbox (Version 6.1.1). For network traffic capturing for analysis, we will use Wireshark, which comes in default with Kali Linux.

In our experimental setup, we will use Eclipse Mosquitto Software [22], a client for the MQTT protocol. It is an open-source and cross-platform MQTT client. The reason to choose Mosquitto is that simultaneously t acts as server and broker. So, it will be easier to generate network traffic in Mosquitto and capture them for analysis. So first, we are installing the Mosquitto server and client in our test environment shown in Figure 4.1.1:

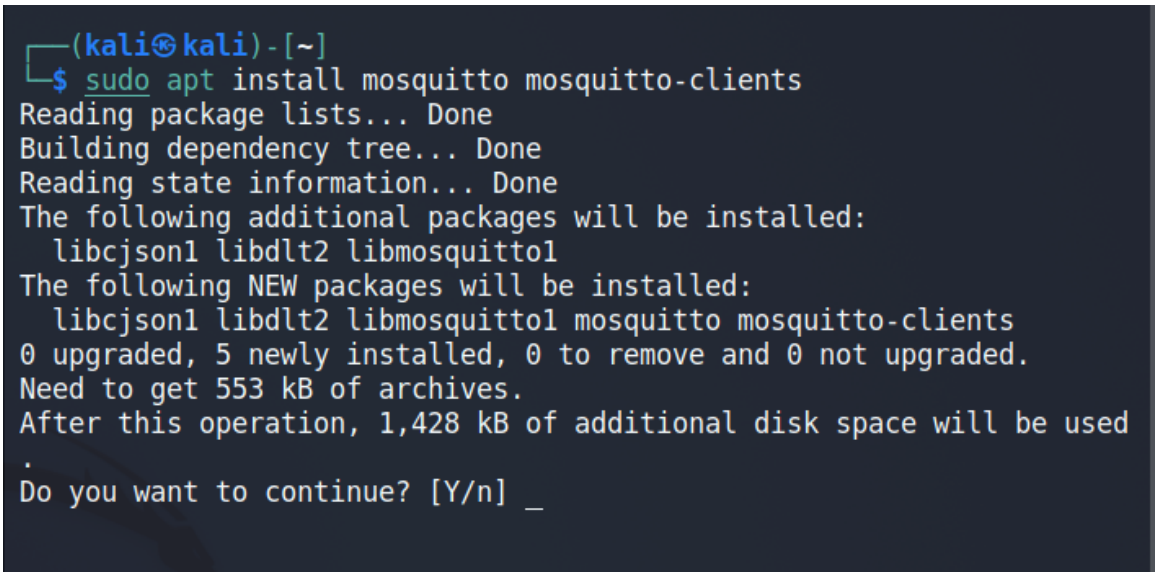


Figure 4.1.1: Installing MQTT clients.

After installing, the broker starts listening on the TCP port. We are starting our server as shown in Figure 4.1.2:

Figure 4.1.2: Starting the MQTT service.

To test the server is working or not, we are trying to subscribe to a topic, shown in Figure 4.1.3:

Figure 4.1.3: Testing the server and broker connection.

We verified that our MQTT environment is working. First, to test authentication security, we have to configure our MQTT server. Next, we have to create a user “test” and set up a password for that user for authentication, shown in Figure 4.1.4.

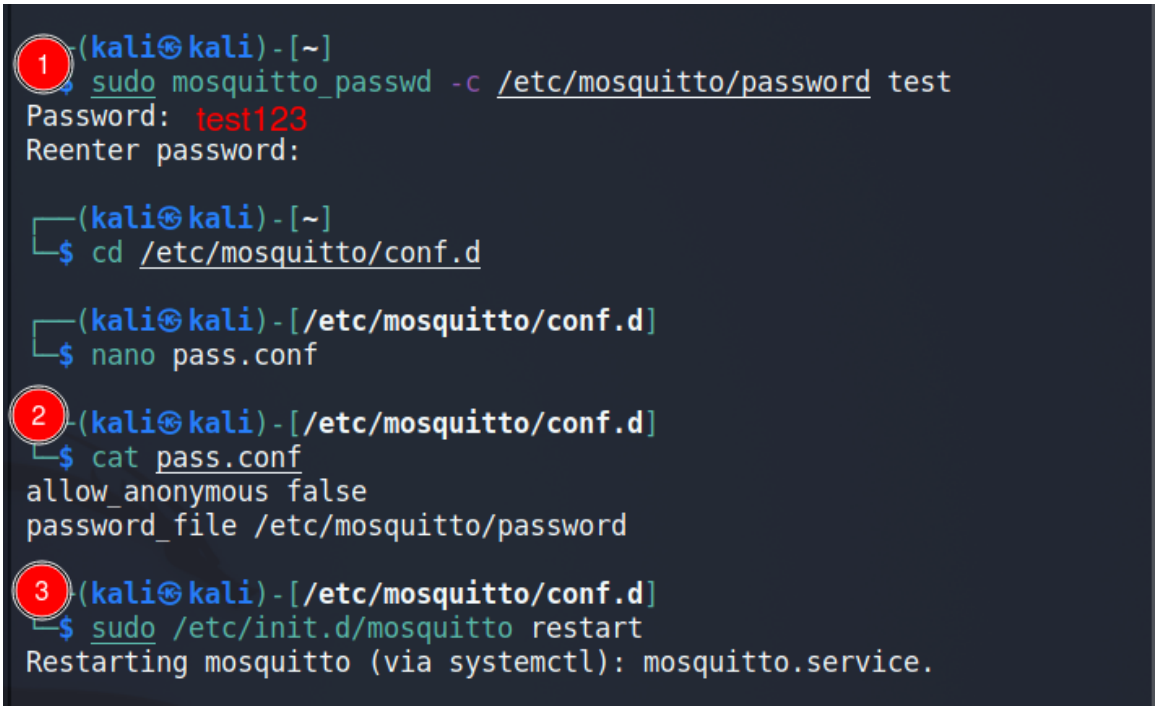


Figure 4.1.4: Configuring the service.

We have created a configuration file for the user in the configuration directory, shown in Figure 4.1.4, by the number 2. After creating the desired configuration file for the user, we restart the server to take effect, shown in figure 4.1.4, by the number 3.

Now, we have the configuration for our desired broker, and it is working, shown in Figure 4.1.5. However, if we try to publish or subscribe in the broker without any valid username and password, we should get an error message.

Figure 4.1.5: Testing the authentication.

We launched Wireshark to capture the network traffic for mosquito protocol. The MQTT broker sends a CONNACK packet to reply to the Connect Acknowledgement and successfully connects to the server. Wireshark captures it, shown in Figure 4.1.6.

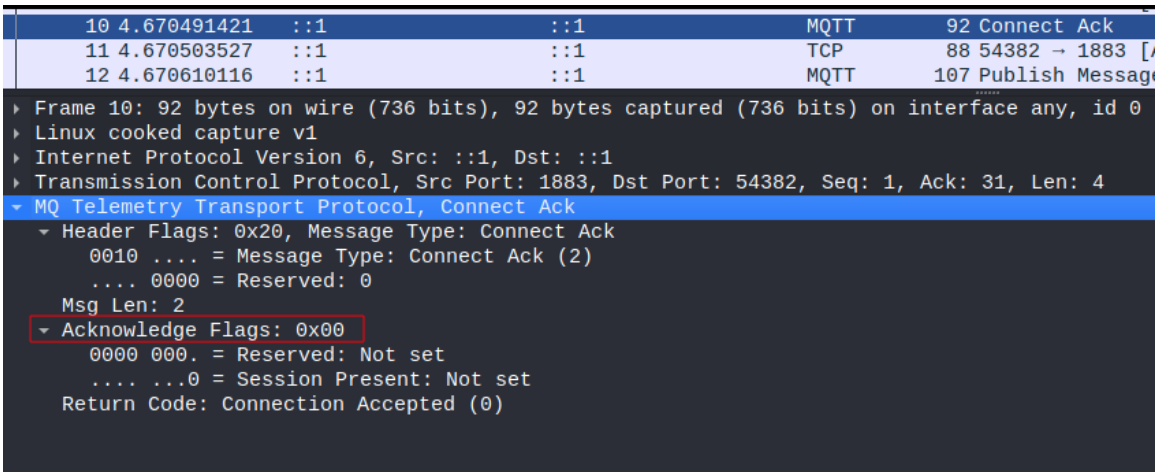


Figure 4.1.6: Captured network traffic of MQTT.

4.2 Experimental Results & Analysis

First, let us look at the structure of the header in the MQTT connection. MQTT packet contains a fixed header [23], shown in table 4.2.1.

Table 4.2.1: The header of MQTT.

Bit	7	6	5	4	3	2	1	0
Byte 1	MQTT Control Packet Type				Flags specific to each MQTT Control Packet Type			
Byte 2	Remaining Length							

There are two types of fields in the fixed header, as we can see here. The first one represents the type of the packet and the second one represents the value of the return code. First, let us the available control packet types of MQTT [23], shown in table 4.2.2.

Table 4.2.2: MQTT Packet Types.

Name	Value	Direction of flow	Description
Reserved	0	Forbidden	Reserved
CONNECT	1	Client to Server	Client request to connect to the server
CONNACK	2	Server to Client	Connect Acknowledgment
PUBLISH	3	Client to Server/ Server to Client	Publish message
PUBACK	4	Client to Server/ Server to Client	Publish Acknowledgment
PUBREC	5	Client to Server/ Server to Client	Publish received
PUBREL	6	Client to Server/ Server to Client	Publish release
PUBCOMP	7	Client to Server/ Server to Client	Publish complete
SUBSCRIBE	8	Client to Server	Client subscribe request
SUBACK	9	Server to Client	Subscribe acknowledgment
UNSUBSCRIBE	10	Client to Server	Unsubscribe request
UNSUBACK	11	Server to Client	Unsubscribe acknowledgment
PINGREQ	12	Client to Server	PING request
PINGRESP	13	Server to Client	PING response
DISCONNECT	14	Client to Server	Client is missing
Reserved	15	Forbidden	Reserved

4.2.1 Authentication

As we configured the client to use an authentication mechanism that uses username and password to authenticate the connection, the MQTT broker establishes the relationship with the CONNECT packet, shown in the table. In response to a CONNECT packet from the client, the MQTT broker sends the CONNACK packet. The CONNACK packet contains the "return code" field, representing the authentication result. All return code values are listed, shown in table 4.2.1.1 [23].

Table 4.2.1.1: Return Code values of CONNACK packet

Value	Return Code Response	Description
0	0x00 Connection Accepted.	Connection accepted.
1	0x01 Connection Refused, unacceptable protocol version.	The server does not support the level of the protocol requested by the client.
2	0x02 Connection Refused, identifier rejected.	The Client identifier is correct UTF-8 but not allowed by the server.
3	0x03 Connection Refused, Server unavailable	The Network Connection has been made, but the service is unavailable.
4	0x04 Connection Refused, bad user name or password.	The data in the username or password is malformed
5	0x05 Connection Refused, not authorized.	The Client is not authorized to connect
6-255		Reserved for future use

For an attacker to act as publisher or subscriber, he needs to know the username and password. An attacker can track down which packets contain necessary information by tracking the return values. Furthermore, if the attacker and publisher are in the same network, they can sniff the traffic. If the username and password are revealed in the traffic, an attacker can take advantage of that information. For example, we have captured

the traffic when the CONNECT packet is sent from publisher to broker to connect, and the username and password are revealed, shown in Figure 4.2.1.1. Thus, an attacker can achieve this information efficiently.

Also, in the authentication process, the header includes the KeepAive header, which informs how long an IoT device is connected with the broker. When the time is expired, the device resends the CONNECT packet to restart the connection.

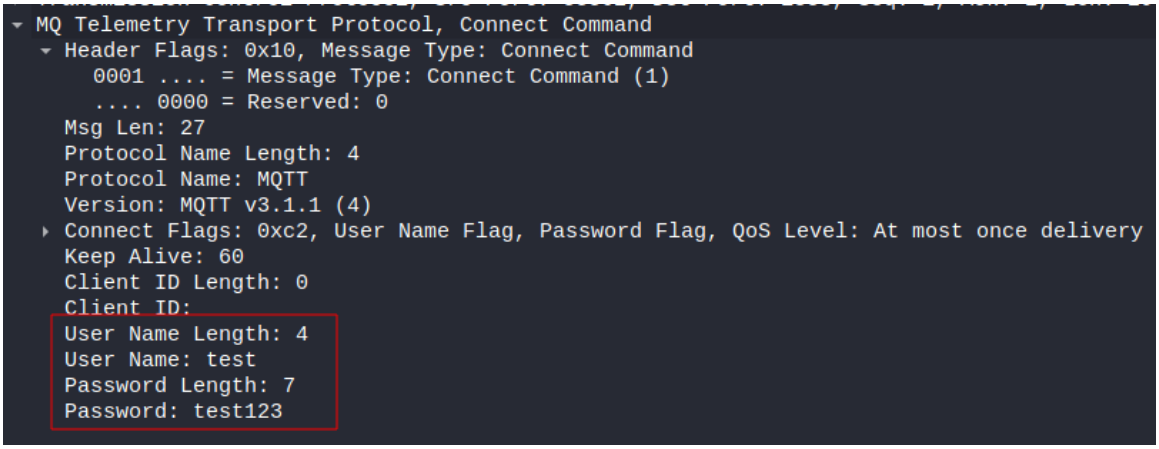


Figure 4.2.1.1: Captured network traffic - authentication.

4.2.2 Data Privacy

Data privacy in MQTT can be considered a significant issue. Whether the broker uses authentication or not, an attacker can still detect the data. For example, in Figure 8, Wireshark captured the data transmitted by the broker, which includes information about message length and Topic, shown in Figure 4.2.2.1.

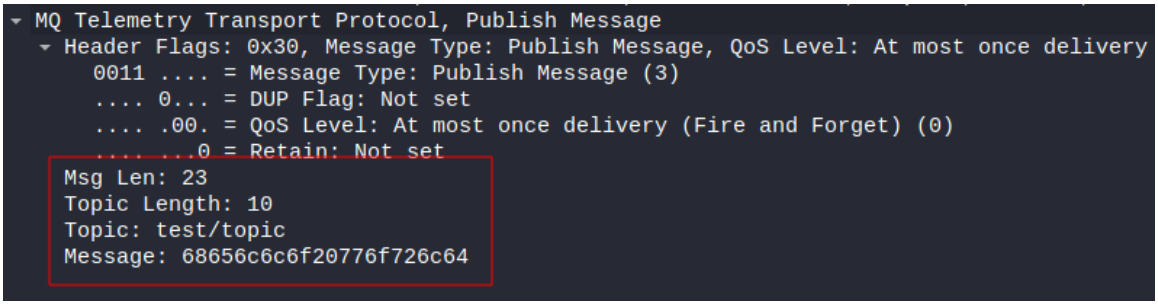


Figure 4.2.2.1. Available information from network traffic.

4.2.3 Data Integrity

Valuable information is exposed in network traffic, and by using Wireshark, an attacker can quickly obtain that information. When an attacker knows about the valuable data packet information, he can modify the data during transmission. By filtering the data from transit, attackers can use Etterfilter [24] (an open-source software) and Ettercap [25] (a network tool used for changing the data) to filter, compile and modify the data.

4.3 Discussion

The header of MQTT is light-weighted, which is also mentioned in the official manual, "MQTT solutions are often deployed in hostile communication environments"[26]. Therefore, it means the header is one of the primary sources of abuse which we have seen in Figure 7 and Figure 8. Furthermore, in the official manual of MQTT security, they have also mentioned some security threats concerning MQTT [26].

- Devices could be compromised.
- Data at rest in Clients and Servers might be accessible.
- Protocol behaviors could have side effects.
- Injection of spoofed control packets.
- Communication could be intercepted, altered, re-routed, or disclosed.

This proves our experiment about authentication, data privacy, and data integrity. MQTT does not have encryption by default. We have to configure our MQTT broker and server to use authentication, which means authentication is optional. It is a significant security issue for MQTT as attackers sniffing the connection can interfere with the data easily. MQTT server with default configuration is an ideal target for breaching, and by accessing the server, attackers can get access to all the messages going through it. Poorly configured MQTT servers are publicly available on the internet, which can be found

through Shodan. Shodan is the world's first IoT search engine for Internet-connected devices. According to Shodan, almost 460000 MQTT servers are exposed on the internet, shown in Figure 4.3.1 (August 07, 2021).

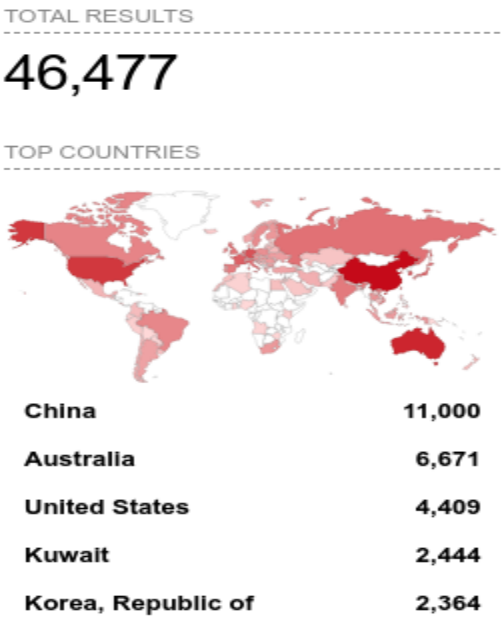


Figure 4.3.1: Exposed MQTT brokers in Shodan.

Kant et al. [27] discussed the security risks of the exposure of the MQTT protocol in detail. Their research paper showed how detailed information is exposed on the internet. They conducted their research using the Shodan search engine and based on the port MQTT protocol using. They predict that the number of devices exposed on the internet could be a double-digit amount in Billions of IoT devices as the uses of IoT devices rise very fast. Furthermore, they mentioned that "standard security mechanisms and hardware protections such as TLS are not feasible, supported, or activated within IoT devices"[27]. IoT appliances are connected to the open internet, and these are the main reasons for exposed IoT devices on the internet.

Joseph et al. [28] also discussed the authorization problem in MQTT in their research. They show that "MQTT over WebSocket allows an attacker to send malicious scripts to the server," which enables the attacker unauthorized access to the MQTT server. In their research, Speh et al. [29] have discussed that the protocol itself does not provide any mechanism to authorize, and the security lies in the broker's hand.

Some attacks are mentioned in the various research papers, journals, articles, and websites dedicated to the IoT world based on this problem. They are:

- Replay attacks
- Denial of Service attacks (DOS)
- Retained Message Attack
- Slow DoS attack
- Man in the middle attack

Chen et al. [30] discussed these attacks in their study on MQTT security. They pointed out that the middle in the man attack is more destructive than eavesdropping attacks and DDoS attacks.

CHAPTER 5
IMPACT ON SOCIETY

5.1 Impact on Society

Providing security to the MQTT protocol is very important compared to all other protocols. MQTT is widely used in healthcare, education, manufacturing, and transportation because of its simplicity and scalability. MQTT has overcome the gap between different protocols so that different devices using the other protocols can communicate with MQTT. Intelligent home systems are being implemented widely, making our lives easier and comfortable. However, security issues on MQTT can expose our home to the open internet. A thief with some knowledge of the protocol can access our home anytime they want and can get a hand on messages going through the networks.

The IoT world suffers from different kinds of viruses from time to time. For example, the wannacry and NotPetya virus attacks caused trillions of dollars of damage globally. The IoT ecosystem is used in critical infrastructure and manufacturing, which has impacted. The consequences of IoT security failures may cause a direct loss of life as they are involved in the healthcare industry. When the wannacry hit, patients with acute conditions were untreated for several days because the virus delayed care delivery for a couple of days.

Hospitals are the most vulnerable sector to IoT security issues. Implanted medical devices that include pacemakers, drug administration devices, monitoring devices, and infusion pumps can have severe effects on health if the IoT device has been tampered with.

IoT devices can also help with DDoS attacks as every IoT device acts as a mini-computer. Less secure IoT devices can be captured easily. By reprogramming them to conduct malicious acts, an attacker can launch a DDoS attack that badly affects service or organization.

5.2 Ethical Aspects

As every modern-day technology uses users' information to process and offers better services, ethical issues are significant in this sector. Privacy and information security are some of the most important among them. IoT companies use different technology to collect data from the user and environment. So, while collecting data, which type of data should be collected or not is an active debate over the years. Also, how companies process and provide security on the data is a topic that should be discussed broadly.

IoT protocols are not only limited to their core design. It also depends on how the protocol is implemented on a specific technology. So, studying and examining the technology to find vulnerabilities is essential to the IoT world. Therefore, security researchers are bound by the law; researching and exploring a technology without proper permission can cause a lawsuit against a security researcher.

5.3 Sustainability Plan

Technology is constantly changing in this modern era. Technologies go through massive development, trial, and error. This development process is so fast that the issue is solved overnight after finding zero-day vulnerabilities. And the update is instantly delivered to all active services over the world. So sustainability plan in this type of research is not so broad. Instead, this research focuses on the security issues that have not been fixed until today and gives awareness to future researchers who will study and work on security issues of the IoT world.

CHAPTER 6
SUMMARY, CONCLUSION, and IMPLICATION FOR FUTURE RESEARCH

6.1 Summary of the Study

With the widespread adoption of MQTT, the attackers continuously exploit and attack this lightweight protocol which meets the needs of light and fragile environments. In this report, we tried to present them and discussed some of the attack vectors for the internet of things. We have shown that authentication, data privacy, and authorization are still significant issues for the MQTT protocol. Nowadays, security vulnerabilities are becoming more common in the IoT world, and the types of attacks are broader than in the past. Also, we have discussed what other researchers have found in their research and what can be done to develop this protocol better.

6.2 Conclusions

The IoT world consists of embedded devices and sensors, and as this technology is portable, small in size, they need a mobile ecosystem and a small, effective solution. To meet the requirements, companies are producing devices without thinking about security. Protocols like MQTT meet the requirements of the IoT world but lack security. Security is crucial for the internet of things as we are very much engaged with these technologies. Any consequences of IoT security failure might cause a direct loss of life. For example, when the wannacry virus hit the internet, many patients with time-sensitive conditions were untreated because the wannacry delayed care delivery for about four to five days.

Providing security to the protocols is necessary because they help the IoT world connect. Therefore, it is essential to protect the IoT-connected devices from attacks and misuse and make them a secure, reliable paradigm.

6.3 Implication for Further Research

This report tried to discuss the security issues of the MQTT protocol and some attack vectors of the protocol. Although the MQTT protocol is not designed with security in mind, researchers are working on making it more secure and proposing solutions and frameworks to make it more reliable. With the knowledge gained from this research, we want to further develop an exploit framework on the existing development of the MQTT protocol. Also, I want to build an automatic detection of CVE vulnerabilities of MQTT. Discovering zero-day vulnerabilities and more research on various protocols, including MQTT, is the main focus of future work.

References

[1] “Global IoT market to grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue.”, available at <<https://transformainsights.com/iot-market-24-billion-usd15-trillion-revenue-2030>>, last accessed on Aug. 03, 2021, at 10:30 PM.

[2] “OWASP Internet of Things Project - OWASP.”, available at <<https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10>>, last accessed on Aug. 03, 2021, at 10:55 PM.

[3] Grant Hernandez, Orlando Arias, Yier Jin, and Daniel Buentello, “Smart Nest Thermostat: A smart spy in your home,” *Black Hat USA*, Aug. 2014.

[4] D. Cooke *et al.*, “Vulnerabilities of the Artificial Pancreas System and Proposed Cryptographic Solutions,” *2020 Undergrad. Res. Showc.*, Apr. 2020, [Online]. Available: https://scholarworks.boisestate.edu/under_showcase_2020/29

[5] “Internet of Things (IoT) - Part 2 (Building Blocks & Architecture).”, available at <<https://www.c-sharpcorner.com/uploadfile/f88748/internet-of-things-part-2/>>, last accessed on Aug. 03, 2021, at 11:20 PM.

[6] System Security Study Committee, Commission on Physical Sciences, Mathematics, and Applications, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, and National Research Council, *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C.: National Academies Press, 1991, p. 1581. DOI: 10.17226/1581.

[7] “Black Hat USA 2015: The full story of how that Jeep was hacked.”, available at <<https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/>>, last accessed on Aug. 03, 2021, at 11:20 PM.

[8] “How to use IoT authentication and authorization for security,” *IoT Agenda*, available at <<https://internetofthingsagenda.techtarget.com/feature/How-to-use-IoT-authentication-and-authorization-for-security>>, last accessed on Aug. 03, 2021, at 11:20 AM.

[9] “IoT Security – Part 2 (101 – IoT Attack surface),” *Payatu*, available at <<https://payatu.com/blog/Admin-Payatu/iot-security-part-2-101-iot-attack-surface>>, last accessed Aug. 12, 2021, at 1:30 PM.

[10] “IoT Security – Part 3 (101 – IoT Top Ten Vulnerabilities),” *Payatu*, available at <<https://payatu.com/blog/Admin-Payatu/iot-security-part-3-101-iot-top-ten-vulnerabilities>>, last accessed Aug. 13, 2021, at 11:30 AM.

[11] M. Lombardi, F. Pascale, and D. Santaniello, “Internet of Things: A General Overview between Architectures, Protocols, and Applications,” *Information*, vol. 12, no. 2, p. 87, Feb. 2021, DOI: 10.3390/info12020087.

[12] S. N. Mohanty *et al.*, “An efficient Lightweight, integrated Blockchain (ELIB) model for IoT security

and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020, DOI: 10.1016/j.future.2019.09.050.

[13] M. Trnka, T. Cerny, and N. Stickney, "Survey of Authentication and Authorization for the Internet of Things," *Secur. Commun. Netw.*, vol. 2018, p. e4351603, June. 2018, DOI: 10.1155/2018/4351603.

[14] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, DOI: 10.1109/JIOT.2017.2694844.

[15] H. Tschofenig and E. Baccelli, "Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security," *IEEE Secur. Priv.*, vol. 17, no. 5, pp. 47–57, Sep. 2019, DOI: 10.1109/MSEC.2019.2923973.

[16] "Security in the Internet of Things," *Wind River*., available at <<https://www.windriver.com/whitepapers/security/security-in-the-internet-of-things>>, last accessed Aug. 05, 2021, at 5:30 PM.

[17] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, DOI: 10.1007/s11276-014-0761-7.

[18] J. Cynthia, H. Parveen Sultana, M. N. Saroja, and J. Senthil, "Security Protocols for IoT," in *Ubiquitous Computing and Computing Security of IoT*, N. Jeyanthi, A. Abraham, and H. Mcheick, Eds. Cham: Springer International Publishing, 2019, pp. 1–28. DOI: 10.1007/978-3-030-01566-4_1.

[19] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture," *Future Internet*, vol. 9, no. 3, Art. No. 3, Sep. 2017, DOI: 10.3390/fi9030027.

[20] H. Bhanujyothi, J. Vidya, S. J. TJ, and D. Sahana, "Diverse Malicious Attacks and Security Analysis on MQTT protocol in IoT."

[21] "Why MQTT Is Essential for Building Connected Cars," *IoT For All*, Aug. 29, 2019., available at <<https://www.iotforall.com/why-mqtt-essential-connected-cars>> last accessed on Aug. 12, 2021, at 5:30 PM.

[22] "Eclipse Mosquitto," *Eclipse Mosquitto*, Jan. 08, 2018. <<https://mosquitto.org/>>, last accessed Aug. 06, 2021, at 4:30 PM.

[23] V. Pasknel, "Hacking the IoT with MQTT," *Medium*, Jul. 19, 2017. , available at <<https://morphuslabs.com/hacking-the-iot-with-mqtt-8edaf0d07b9b>>, last accessed Aug. 15, 2021, 8:40 PM.

[24] "etterfilter(8) - Linux man page.", available at <<https://linux.die.net/man/8/etterfilter>>, last accessed Aug. 07, 2021, at 6:15 PM.

[25] *Ettercap/ettercap*. Ettercap Project, 2021, available at: <<https://github.com/Ettercap/ettercap>>, last accessed: Aug. 07, 2021, [Online] at 10:55 PM.

[26] "5 Security (non-normative).", available at

<<https://docs.solace.com/MQTT-v50-Prtl-Conformance-Spec/mqtt-v50-5-security.htm>>, last accessed Aug. 07, 2021, at 10:30 PM.

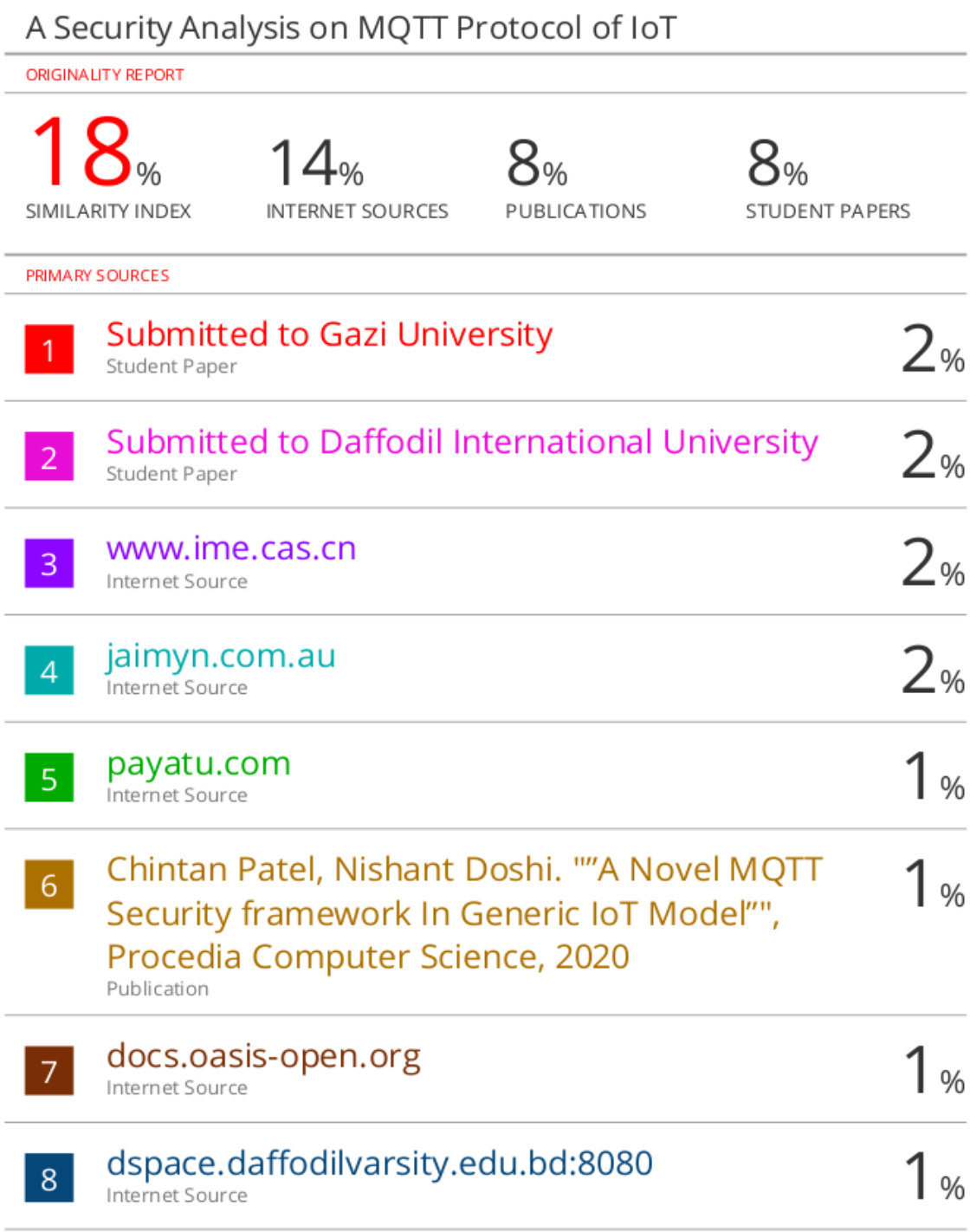
[27] “Analysis of IoT security risks based on the exposure of the MQTT protocol,” Jan. 18, 2021., available at <<https://www.ingentaconnect.com/content/ist/ei/pre-prints/content-ei2021-mobmu-096>>, last accessed Aug. 07, 2021, at 11:30 PM.

[28] J. J. Anthraper and J. Kotak, “Security, Privacy and Forensic Concern of MQTT Protocol,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3355193, Mar. 2019. DOI: 10.2139/ssrn.3355193.

[29] I. Heđi, I. Špeh, and A. Šarabok, “IoT network protocols comparison for the purpose of IoT constrained networks,” in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2017, pp. 501–505. DOI: 10.23919/MIPRO.2017.7973477.

[30] F. Chen, Y. Huo, J. Zhu, and D. Fan, “A Review on the Study on MQTT Security Challenge,” in *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, Nov. 2020, pp. 128–133. DOI: 10.1109/SmartCloud49737.2020.00032.

Plagiarism Report



A Security Analysis on MQTT Protocol of IoT

ORIGINALITY REPORT

18%	14%	8%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Gazi University Student Paper	2%
2	Submitted to Daffodil International University Student Paper	2%
3	www.ime.cas.cn Internet Source	2%
4	jaimyn.com.au Internet Source	2%
5	payatu.com Internet Source	1%
6	Chintan Patel, Nishant Doshi. ""A Novel MQTT Security framework In Generic IoT Model"", Procedia Computer Science, 2020 Publication	1%
7	docs.oasis-open.org Internet Source	1%
8	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%