A Survey on Man-In-The-Middle Attacks in IoT Devices

Bharath Mukka
Department of Comouter Science
University of Missouri-St. Louis
St. Louis, USA
bmkcq@umsystem.edu

***Abstract*—Man-In-The-Middle-Attack (MITM), a well-known type of attack in the Internet of Things (IoT) and computer communication. In this attack, an attacker targets the data flow between the two communicating parties and tries to intercept the data by compromising its confidentiality and integrity. This attack has the capability to enable an attacker to direct the internet traffic to flow through the attacker machine. This survey presents explanation on some of the existing MITM attacks, weaknesses that led to MITM attack, statistics and some counter measures with a discussion between each type of weakness among the IoT devices.**

Keywords— Man-In-The-Middle (MITM), Internet of Things (IoT), Bluetooth Low Energy (BLE), MQTT (Message Queue Telemetry Transport) Protocol, CoAP (Constrained Application Protocol), RFID (Radio Frequency Identification), HTTP (Hypertext Transfer Protocol)

I. INTRODUCTION

In today's world, almost each and every human on this planet is associated with the cellular or internet network usage. At present IoT is playing a major role in the internet network and these devices can be found everywhere. They are mainly used to fulfill the needs of industrial automation and human beings in the form of smart homes with automated detection and controlling of lights, air conditioners, entrance doors, baby monitors, Sensors embedded in rest rooms for water and power management, music players, health monitoring devices, smart robots in industry and much more. All of these devices are connected to internet in some form or the other and involve in confidential data exchange mechanisms.

Security in IoT devices is an essential part in present day world. As these devices growth is rapid, the data flowing in the network is also increasing at a rapid pace by leaving a huge confidential data into the hands of attackers. These attacker pose threat to human life and industries in which IoT devices play a vital role. The attackers keep on attacking until some useful information is found and as a result brand new attack methodologies are coming into existence in the market. One of the well-known attack types is Man-In-The-Middle attack (MITM).

MITM is a kind of attack where an attacker eavesdrops to the communication between two end points, here the end points may be one system communicating with the other over the internet or cellular network. The attacker impersonates both the

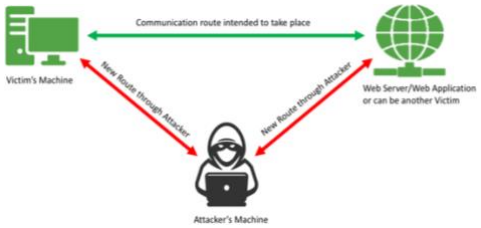

Figure 1: Man-in-the-Middle Attack scenario

communicating parties and gains access to the data flowing between the parties and tries to send, receive, or intercept this data which is meant for someone and steal confidential data related to health, banking, home controls, etc. Figure 1 clearly depicts the MITM attack.

The primary cause of this attack is due to lack of features implemented for security. Now-a-days there are many manufacturers building new and advanced technology involving IoT devices at a very fast pace, low cost and those solve the real world problems, but at the expense of security. The reason I chose MITM is because it gives an attacker a large mark of liberation to manipulate the communication between sender and receiver with read and write access to very sensitive information and it goes unnoticed by the communicating parties.

The survey in this paper addresses various types of MITM attacks related to emerging IoT technologies, reasons behind these attack types, MITM attack statistics and some mitigation techniques to implement in IoT devices.

II. HISTRORY OF MITM ATTACKS

MITM attacks came into existence before the computer era, a typical example could be a malicious postman opening the letter in an attempt to read or change its content before giving it to the recipient [1]. Later when the internet came into existence and communication between the computers started, the MITM attacks advanced in much more technical ways by exploiting the vulnerabilities in the network protocols and caused a huge loss to confidentiality and integrity between the communicating parties.

Even though people started discovering these devices from 1980s, the "Internet of Things" was termed in the year 1997, but the actual matured devices came into light after 2005 and took a major role in automating the world connected to internet.

Unlike ransomware or phishing attacks, the MITM attacks are not much common but are kind of ever present threat to the organizations. MITM attackers use different techniques for intercepting the communication between two communicating nodes. Section IV in this survey describes some of the MITM attacks on IoT devices in detail.

III. IOT ARCHITECTURE AND MITM ROOT CAUSE

As most people are well aware of traditional TCP/IP layered architecture in the internet and computer networks, IoT also involves in something kind of a layered architecture with 3 layers namely Application layer, Transport layer and a Perception layer as illustrated in Figure 2. Note: There are some articles which represents four layers in IoT architecture as Application, Perception, Network and Physical layer. This is mainly due to various kind of devices and high heterogeneity among them. In this paper three layered architecture is considered.

Here, Perception layer is the main layer about collecting and analysing data collected from different perception nodes [2]. This is divided into perception Node(controllers, sensors, etc.), and Perception Network(for communication with transport layer).Transport layer provides ubiquitous access environment for perception layer to store and transmit information [3]. Application layer is a kind of an advanced layer present above the transport layer and supports technologies related to Middleware, cloud computing, Information development and service support platforms. This layer is used to establish the connection between users and devices with the information collected from perception layer and this layer can be organized as per the services requirement and access control design strategies [3][6].

A. Architectural Issues in Transport Layer:

This is the layer responsible for making transmissions reliable with information and data communications [6]. As this layer contains access network, core network and local network and this is the layer where devices are connected to internet as shown in Figure 2, MITM attacks are one of the many attacks those begin at the transport layer/ network layer. MITM attacks fall under "Gateway and Internal network" category of IoT attacks [4]. These gateways and internal network devices at this layer are used in networking and routing information and data packets to the destination. Attack usually takes place while forwarding data form one layer to the other or to another device connected to the network.

There are a number of ways MITM attacks can occur, the mode of attack mainly depends on the path chosen and the goal of attacker. If the victim uses wireless as the mode of communication, then the attack is done by using wireless attack methodologies like ARP (Address Resolution Protocol) poisoning. ARP poisoning is the main weakness point in the communication where an attacker can route the traffic between the communicating entities through his/her machine. ARP spoofing attack techniques and mitigations explained in detail at [5].

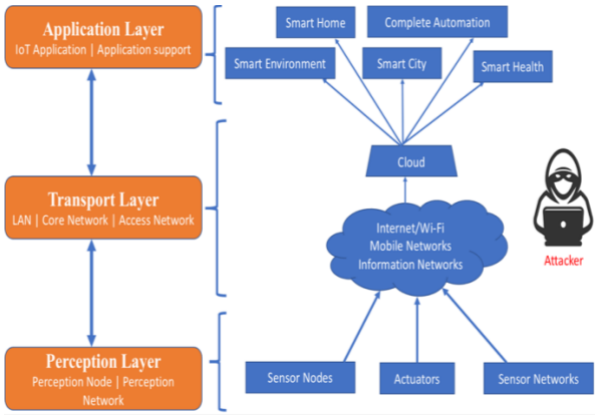

Figure 2: IoT Layered Architecture and possible MITM area of attack

IV. MITM ATTACKS

With the ever-growing number of IoT devices, their integration with the human life in the current world, and due to their various benefits and blunt security features - the number of attacks on these devices are increasing exponentially, MITM is one among these attacks. To become a Man-in-the-Middle, attacker uses some common techniques involving ARP Poisoning, Wi-Fi Eavesdropping, DNS poisoning for some devices, if the IoT device is capable of web browsing then the attacker may use HTTP/HTTPS Spoofing or Session Hijacking. This section describes some real life and educationally implemented MITM attacks.

In the below sub sections, this survey explains some of the emerging technologies in IoT and how they are related to cause MITM attacks. Technologies and protocols mentioned below are discussed in detail in this section.

- BLE (Bluetooth Low Energy) technology.
- MQTT (Message queue Telemetry Transport) protocol
- RFID (Radio Frequency Identification) technology
- Web based attacks, especially due to HTTP (Hypertext Transfer Protocol) and
- CoAP (Constrained Application Protocol)

A. BLE Technology and its Relatalbility to MITM attack

The BLE (Bluetooth Low Energy) also known as the Bluetooth smart is one of the major communication protocols implemented in many smart devices like smart wearables, medical appliances, and much more [8]. BLE is implemented at the Data link layer and most of the IoT devices in today's world using this BLE protocols lack a lot of security measures which in turn lead to major security issues. The Bluetooth technology was first introduced by Nokia in the year 2006, using this as the base technology, BLE is designed and became main Bluetooth standard for almost all smart devices. The main goal for designing Bluetooth low energy standard is to enhance for short-range, very low latency and bandwidth with fast transmission, and these include Physical and Mac layer for in-vehicle networking [12].

Table 1: BLE characteristics [13][14]

Bluetooth Low Energy (BLE) Characteristics	
Standard	IEEE 802.15.1
Topology	Star-Bus Network or scatternet
Data Rate	1 mbps
Latency	~ 6ms
Range	Short Range ~15 to 30 m, some support ~100 m
Frequency	around 2.4 GHz
Encryption Standard	AES-128 Bit stream
Network	WPAN

BLE works on the basis of master/slave architecture and it offers advertising and data frames. Where advertising frames/channels are used to send beaconing packets which are in-turn called as Advertising packets. Master node senses these channels to find slaves and connect to them, once the connection is established data starts flowing between them [12][14]. Further information on BLE communication and pairing process can be found at [13][15][16]. Table 1 represents BLE characteristics commonly used in the IoT communication.

As Bluetooth smart plays a major role in IoT communications, till BLE 4.0 and 4.1 versions these devices do not perform error correction but can only does error detection, and there are many IoT devices in the market which are operating on BLE version 4.0 or less. Due to this reason, many devices are becoming prone to MITM attacks. Taking this as an advantage unsecured firmware upgrades, re-routing the packets, disconnecting the smart devices with the mobile, eavesdropping, integrity theft, and many kind of attacks were happening on these IoT devices.

There are two kind of attacks that are possible on these devices, one is Passive interception and the other is an Active interception. Let's see in detail about these two attack types

Passive Interception: In this type of attack, the attacker does what is known as eavesdropping, this interception can be done in many ways if there exists some improper encryption and no authentication between the communicating parties. As there is no proper implementation of encryption, attacker can easily capture all the packets flowing from and to the device using some opensource tools like Wireshark, BtleJuice, and etc..

Active Interception: In this type of attack, the attacker not only does eavesdropping but also intercepts the communication and alter the data transmission between the devices or device and its application by compromising the integrity of communication. In general scenario, active Interception attacks are referred to as MITM attacks, but passive attacks could also be MITM attacks and these active attacks depend on the type of data that is flowing between the communicating parties.

Recently in 2020, a flaw in BLE devices ranging from version 4.0 to 5.0 is identified and lead IoT devices to MITM attacks. This flaw allowed attackers in wireless range to bypass the authentication keys and lead to passive or active interception attack. This high-severity vulnerability is termed as "BLURtooth", CVE-2020-15802 [33] discovered this in the Bluetooth (v4.0 to 5.0) pairing process and termed this pairing as CTKD (Cross-Transport Key Derivation), explains this in detail along with mitigations. BlueBorne attack exploitable can also lead to MITM. Even as the new and secure implementations keep on emerging in the current world, the researchers are also in lookout for flaws among the newer versions and making it secure day-by-day, although cent percent security is never guaranteed.

B. MQTT Protocol and its Relatability to MITM atacks

MQTT, short for Message Queue Telemetry Transport Protocol is one of the light weight application-layer protocols which aims to connect devices and network with middleware and applications, using the concept of Subscribe, Publish, and Broker. It uses TCP or UDP depending on the functionality that it is designed for. In the concept of this protocol, security here is achieved by the broker, it checks for the authorization of the participating entities with the help of username and password before the establishing a connection and the payload here is encrypted [26]. Publisher here is used to publish a message to one or many topic in the broker, Subscriber will subscribe to one or many topics present in the broker and are able to receive messages from publisher, routing of message from publishers to the subscribers is done with the help of broker and the levels in broker are separated by topics, an example topic is 'smart house/bedroom/lights' the levels are separated by a forward slash for better representation [40].

This seems like one of the most secured protocols, but MQTT is not initially designed for keeping security in mind, traditionally this is used in the back-end network for some specific application purposes with minimal features of authentication and interoperability built into this protocol. The username and password are transmitted in plain text and may not be secure without transportation level encryption. However, it restricts the broker access with some form of authentication. As broker here does packet analysis and forwarding, there needs to be a lot of packet filtering mechanism that needs to be implemented at the broker level, because some malformed packets from subscribe or publish leads to exploitation issues at the broker level and all the communication may get decoded and taken by an attacker [9]. MQTT is also becoming more and more secure day-by-day and is now became an ideal messaging service for IoT devices and is most suitable for home automation of IoT.

MQTT on its own does not have a developed security mechanism, but it mostly depends on SSL/TLS for encrypting these messages [9]. On the other hand, due to the resource and manufacturers constraints, it is not totally enforced in IoT devices. In [9] it presents an MITM attack on IoT devices on MQTT protocol and using BERT (Bidirectional Encoder Representations from Transformers) based adversarial message generation, where the ratio of port scanning results from scanning port:1883 (default MQTT port) and port:8883 (SSL/TLS port for MQTT) is considered to be around 12625:1, which leaves room for serious security vulnerabilities in IoT which are based on MQTT protocol. Reference [9] clearly explains how this vulnerability leads to MITM attacks, how it can be exploited and the outcomes of the attack.

An official note from mqtt.org on v3.1says "*You can pass a user name and password with an MQTT packet in V3.1 of the protocol. Encryption across the network can be handled with*

SSL, independently of the MQTT protocol itself (it is worth noting that SSL is not the lightest of protocols, and does add significant network overhead). Additional security can be added by an application encrypting data that it sends and receives, but this is not something built-in to the protocol, in order to keep it simple and lightweight." [27].

With the rapid growth in IoT device utilization, manufacturers of these devices making authentication an optional or using unencrypted/poorly configured authentication. Which leads to MITM attacks which can be executed to steal passwords. MQTT protocol with the advancements from version 3.1 to 5.0, the security of the protocol is given an upper hand by implementing enhanced authentication and authorization techniques where it provides a mechanism to enable authentication in response/challenge style and also includes mutual authentication, along with this, there are some observed performance improvements, restrictions on maximum packet size, adds user properties to most of the packets from server, sender and receiver, enhancements for scalability and improved error reporting [27]. References [29 to 31] gives a brief on the use of MQTT in M2M and IoT, Intrusion detection system for MQTT, and how the MQTT is used with Real time communication services. [32] gives an insight on the vulnerabilities and limitations on previous versions of MQTT protocol, section 5 in this survey also includes some common misconfigurations and mitigations techniques involved in MQTT versions. The newer version in-turn allows SASL (Simple Authentication and Security Layer) style authentication if both server and client supports it and also includes the ability to re-authenticate with in an established connection, thus making MQTT somewhat more secure and less prone to MITM attacks.

C. RFID Technology and its Relatability to MITM atacks

Radio Frequency Identification, in short RFID is one of the most used technology in present day life and has become an industrial revolution in identifying individuals, objects, and has large application in medical sciences, the RFID is a wireless 'tag' which is a combination of a chip and an antenna, this antenna is used in sending the necessary information signals to the RFID reader. RFID reader on the other hand, converts the radio signals received from the antenna into the digital signals and then sends the data to a computer or a processing device for analyzing the information. This technology has completely become an alternative to native technologies like the bar code system.

Apart from some of the superior features in RFID technology like range, accuracy, automation of data collection, enhanced inventory control, and smart shelving [17][18] there are also significant downsides/limitations like privacy, transparency, cost, integrations, and the bigger one i.e., security.

Figure 3: RFID architecture showing communication between Reader and Tag

As this section mostly concentrates on MITM attacks in IoT systems using RFID technology, security and privacy is considered as the major issue here. One of the main security threat which lies in these devices is at the communication between the tags and RFID readers, the figure below shows this communication in IoT embedded with RFID in detail.

Here the possibility of MITM attack considering just the RFID communication is at the exchange of data and sometimes between the RFID reader and Central database. Due to some unsecure protocols for authentication and privacy in the older generations of RFID technology, the attackers are able to easily capture and sniff the data between the communicating parties (Reader, database and tag) as shown in the figure 3. From the past decade, many researchers have proposed various secure protocols and standards to resolve the security issues that are mainly related to authentication and privacy, which in turn might lead to possibility of MITM attacks on these devices [19], in [20] hash functions are used along with time stamps in order to achieve mutual authentication, in [21] pseudo random number generator (PRNG) is used in combination with hash function and Exclusive OR operation, in [22] it uses some random numbers and multiplier functions that are truncated, in [19] light weight authentication protocols are introduced for RFID security, likewise in the recent years, EPC Class-1 Gen-2 (C1G2), combination of protocols with many hash functions for improvising the confidentiality and integrity, EC-RAC family, ECC solutions for security and privacy have been evolving from year to year but the attackers on the other hand kept on finding the loopholes in these protocols/standards and exploiting them. Solutions to these problems can be found in some of the recent published articles on RFID protocols, for example [23 to 25].

However, there will always be a great need to secure the communication between the tag and the reader/server in the RFID architecture.

D. HTTP and its Relatability to MITM atacks

With the ever growing number of IoT devices in both the business and consumer area, The device is mainly characterized by its interconnectivity, dynamic changes, and heterogeneity at a large scale [34]. Hypertext Transfer Protocol (HTTP) is one of the very prominent and common protocol on which IoT devices rely upon, this is an application level protocol and is used in many of IoT devices that use internet to publish/transfer a lot of data. HTTP might lead to various forms of MITM attack like active eavesdropping, ARP or DNS poisoning, Command injections, SSL striping, and many more.

As these IoT devices are resource constrained, HTTP on these became a huge protocol overhead and performance of the devices is degrading significantly, which in turn leading these devices to some serious problems like delays in packet delivery and increase in network resource consumption [35]. HTTP in general operates on TCP/UDP and provides reliable communication between server and the user. Unlike MQTT which is designed for lightweight architecture, HTTP is a kind of symmetric protocol designed for general computer communication.

As the resources on IoT can easily be exhausted, it unlike in normal internet communication, the communication to and from IoT devices on HTTP and with weak authentication can easily be sniffed and analyzed by an attacker. To target an application, attackers perform an MITM attack by easily redirecting the original traffic flow with the technique of ARP poisoning and DNS poisoning. The resources on IoT devices can easily get flooded and leads to heavy data leakage causing financial and personal losses to a great deal.

Most of the manufacturers who are manufacturing IoT devices at present, do not focus much on how the device is communicating and exchanging data, many IoT devices have no mechanism even to verify the certificates and even if certificate verification is implemented, they can easily accept any self-signed certificates from attackers and thinks it as a legitimate one. By implementing certificate trust mechanism, closed HTTP servers, encrypting GET and POST methods, and both the server and client authentication during communication over HTTP can stop MITM attacks to a very large extent.

Script Injection attack also takes place in the same way and especially when the IoT devices are running on an HTTP server with no implementations of authentication, the GET and POST methods are used in identifying the end points of communication and makes attacker's task easy in capturing packets from devices. Now that the attacker knows where and how the communication is taking place, he/she can inject some form of script for example, JavaScript can be injected [36]. When the adversary is hosts this JavaScript on a TLS web server, it can be loaded onto both HTTP and HTTPS sites without any error. When the victim clicks on the received links or ads, malicious code will be executed on the system and then the machine gets completely compromised. This also come under an MITM attack and in general called an active eavesdropping attack.

In order to overcome the overhead problems in HTTP, now-a-days MQTT protocol is being deployed in almost all the IoT devices, but there is also a need for HTTP in some scenarios. [35][38][39] gives a full comparison, usage in IoT, performance evaluation and vulnerabilities in both HTTP and MQTT protocols.

As these attacks present many challenges to the security researchers, these can be detected by using the technique of static signatures [37] i.e., by placing these signatures in many fields of HTTP request. [37] presents many statistics on 'HTTP attacks on Home IoT devices', it also presents many attack scenarios, kind of possible attacks, which country is playing a major role in these attacks, percentage distribution of attacks along with some detection and mitigation techniques. Some of the best possible mitigations are, to implement privacy-focused browsers by limiting the access to private addresses, HTTP end-point security, installing local dnsmasq, making manufacturers more aware of header validation techniques, implementing least privileges in IoT device browsers, keeping IoT devices updated at least on the services that are mostly exposed to the internet [36][37]. By following these detection and mitigation techniques, most of the MITM attacks on IoT devices using HTTP can be reduced to a significant amount.

E. CoAP Protocol and its Relatability to MITM atacks

Like MQTT and HTTP, CoAP also an important and evolving protocol in the IoT and IIoT world. It is one of the web transfer protocols from application layer and is defined in RFC 7252. Unlike MQTT where communication is one-to-many or many-to-one or many-to-many, CoAP is a one-to-one lightweight M2M protocol for transferring data or information between the client and the server and unlike HTTP it's mainly designed only for communication in resource constrained low powered devices and is widely used in wireless sensor network nodes [43]. In the CoAP model, client interacts with the server and server responds to the client and this functionality is achieved by what are known as method codes or response codes, it uses tokenized options to match response to the request and there is a unique message ID for each of these matching responses [43]. CoAP in general works on the REST (Representational State Transfer Model) where an URL is used to access resources but client however makes use of these resources using standard HTTP methods.

CoAP is protected by DTLS (Datagram Transport Layer Security), which runs on UDP (User Datagram Protocol) to enable application-level communication for things RFC 7252 clearly explains how DTLS is implemented for CoAP[44] .

Although there are many security features in place for CoAP, there are still many attacks going on like in MQTT, and MITM is one of the major security issues in CoAP which leaves attackers a way to attack types such as sniffing, DoS(Denial of Service), spoofing, cross protocol attacks, replay and relay attacks [43]. In order to lunch an active interception, a proxy system is installed to the client side in the client-server model [45].

MITM attackers mainly target the two protocols i.e., MQTT and CoAP to intercept the communication between the communicating parties and to steal the message and credentials that are transmitting between them. This leads to sensitive data exposure and some of the main reasons may be unsecured networks, weak web interface by CoAP and other protocols, flimsy implementation of encryption mechanisms, spiteful software updates or no updates in some devices, and using outdated or older versions of security protocols [43]. Even after addressing many of these issues in CoAP through DTLS binding, fragmentation of messages, implementing slicing to reduce the amplification factor, end-to-end encryption and authentication, attackers are still finding ways to intercept the communication and perform MITM attacks. A part of section V explains some common misconfigurations and mitigation in CoAP and its involvement in MITM attacks.

V. MISCONFIGURATIONS AND MITIGATIONS OF IOT PROTOCOLS RELATED TO MITM ATTACKS

With the growing popularity of IoT in Home and Industrial automation, they are becoming prone to cyber-attacks and there is a great need for a challenging approach in achieving the desired security [12]. This section mainly concentrates on BLE, MQTT and CoAP protocols in IoT. One of the main reasons for MITM attack occurrence is due to improper or no use of encryption. These attacks can be mitigated if we prevent the attacker from intercepting the communication among the communicating parties by implementing strong encryption, authentication and authorization techniques, also these attacks must be detectable through these encryption measures, but many IoT software developers and manufacturers fail to properly implement these secure features, which in turn is leading to loss of confidentiality, integrity, and non-repudiation in IoT communication.

As already mentioned that MITM attacks occur due to the misconfiguration in protocols with unsecure configurations, like misconfigurations in BLE, MQTT, RFID, CoAP, HTTP, and etc., lead to MITM attack. Below section from A to D contains detailed explanations of these.

A. BLE Misconfigurations and Mitigations

Misconfigurations: Compared with other security protocols, MITM can easily be deployed and performed on devices using Bluetooth as the medium of communication. Up to BLE version 4.1 they have many vulnerabilities and weak encryption methods with no proper encryptions schemes implemented in IoT devices. As we are now aware that an attacker achieves MITM privileges during the set of pairing strategies in Bluetooth smart devices, the point here in IoT is weak support protocol for mutual authentication that exists between the communicating parties is one of the causes of this attack. Poor encryption schemes at the connection initiation and during the communication process, credential transferring, poorly configured mechanism to identify the status of neighbouring devices, loopholes in passkey entry modes (Example:CVE-2020-10134) and 'Just Works Mode' in many Bluetooth devices makes them pair with other devices without any password or cryptographic protection are some other reasons causing MITM and many other attacks in IOT devices.

Mitigations: One of the main and important technique is to secure the authentication process at the start of communication, having this ensures that they are communicating with the one they are intended to. As most of these BLE devices are deployed in public, it's better to implement this authentication at the application layer using public key cryptography so that it becomes a good defeat to both the downgrade and MITM attacks between the two communicating/pairing devices. Pairing requests are to be accepted only with user interaction so that these attacks can be reduced to a great level, implementing firmware encryption, rejecting unknown requests right away, updating the device firmware from time to time and enabling auto update option if available and updates are to be accepted only from the original device and operating system manufacturer, implementing service restrictions and data exchange on some sensitive applications when BLE device gets paired will reduce the MITM attack surface for the attackers. There are some BLE devices which do not have any authentication and gets paired on the basis of pairing device's name, this should be avoided completely, whenever the manufacturer find themselves or anyone reports any bug or misconfigurations in BLE device, it should be reported to all the users in a very less amount of time and should take proper measures to protect and fix them without causing any loss to users' sensitive data. Upon doing all these, users should be made aware of the technology and how it may lead to attacks.

B. MQTT Misconfigurations and Mitigations

Misconfigurations: As MQTT is one of the widely used communication protocol in IoT and Industrial IoT and is based on publish-subscribe protocol, there are many misconfigurations that are observed from previous versions to the current versions of MQTT protocol. Some of them are discussed here in this section. Most of the MQTT protocol enabled IoT devices are reachable from the public facing servers, which enables MITM attackers to connect to the device from anywhere and steal sensitive records related to user or any organizations (i.e., form Industrial IoT devices). Many manufacturers are deploying IoT devices and MQTT servers with no passwords or password protections into the market and they are becoming prone to many kind of attacks including MITM and attackers target user data by easily establishing communication with any device having this vulnerability and it sometimes allow invalid data supply by malicious clients. The same things also apply to the MQTT servers, the above section on MQTT in this survey describes how vulnerable MQTT servers are and their statistics.

When there are no secure configurations or when IoT devices using insecure and default MQTT configurations, it becomes an easy task for MITM attacker to access all the messages flowing through the established connection, this can be done by using # as a wild card and by subscribing just to # and nothing else can lead access to the communication, so that MITM attacker can perform passive or active eavesdropping attack [41] and also due to these wildcards and linked resources in MQTT can be turned against the users of IoT devices. Unsecure endpoints can also expose confidential records to attackers. Due to these misconfigurations in MQTT enabled IoT devices, telemetry data can be exposed via brokers and this data may include information regarding manufacturing process, kind of generated event requests, and control system names. Due to this type of misconfiguration in one device, may lead many devices prone to MITM attacks. Attackers can also be able to flood clients by sending same message over and over using message retain and modifying Quality of Service (QoS).

In general/common cases, these misconfigurations lead to, connecting to an unprotected smart hubs, subscribing to topics in wildcard, access to files which are protected on MQTT server, and sometimes the MITM attacker can also trace the device location of the user

Mitigations: Similar to Bluetooth, MQTT is a widely used protocol in the communication process for exchanging short messages, and there is no particular format of data that is transported and can be used to transport any data/payload as communicators wish to and a single message can be sent to one or many subscribers to a specific topic. Form this it can be assumed that, one malicious payload sent from one publisher

can lead to compromise of too many subscribers and lead to huge loss related to personal or organizational sensitive data. MQTT and CoAP are similar in most of the cases, but MQTT takes a bit upper hand in support for resource constrained devices.

Implementing data/payload checking mechanisms to verify what kind of data is flowing through the systems and checking for malicious code, executables, and performing data validation on the connected devices during data transport will ensure these devices to become more secure. As discussed, manufacturers should play a vital role in paying high attention to security of IoT and Industrial IoT devices when implementing protocols in them, there are many solutions that already exist to mitigate and overcome MITM attacks in devices using MQTT protocol, but security teams or developers no not employ all these solutions in M2M communication due to some budget issues or lack of awareness. By performing proper testing and risk assessments before the device gets deployed into the market will ensure security of the device and in turn attack mitigation is achieved to some extent. Installing anti-malware programs to detect unusual traffic by providing real-time protection against viruses, malwares, it helps in scanning all incoming data from any network, blocks malicious software, protects from credential theft and interception of communication by MITM attackers. [42] gives a complete idea on how the Keyed-Hash Message Authentication Code (HMAC) works in MQTT and how the authentication and integrity is achieved during the communication process.

Regular security updates and password policies are an important requirement in order to prevent IoT devices from all kinds of attacks. SSL/TLS and X.509 certificate authentication usage in MQTT provides a secure channel for communication between the connected devices and helps overcome the problem of MITM attacks. Having separate network for IoT devices may be useful in mitigating these attacks, but it's quite hard to implement and the same kind of scenarios might as in the general computer networks. Proper implementation of Access Control List (ACL) will be another important mitigation techniques, ACL is a mechanism performed by brokers for access authorization, and it helps in thinking on which device to be connected to, when and on what basis the connection establishes, and this helps in preventing external or unknown connections to the IoT device thus providing protection against MITM attacks. As discussed in MQTT section about SASL authentication, re-authentication with in an established connection will check and ensure that there is no MITM attacker listening to or causing integrity loss to the communication.

C. CoAP Misconfigurations and Mitigations

Misconfigurations: Having said CoAP is an adaptable, light weight, an M2M protocol which connects a vast number of devices over the internet, and which is designed for resource constrained devices. There are many security vulnerabilities discovered by malicious attackers and researchers, and the misconfigurations applied to MQTT will mostly be also applied for CoAP. Due to its rapid growth in the IoT and IIoT and involvement in huge data exchange over the internet, there is not any surprise that these are becoming prone to MITM attacks in the current and may also happen in future too. Manufacturers and developers not paying in detailed attention to the security protocols or giving least importance to security while in its development stage is the bigger problem for a device prone to MITM attacks.

With the involvement of amplification feature, memory leaks found in the CoAP library, weak encryption schemes, unsecured datagrams and the optional authentication feature in one of the communicating parties can lead to MITM attacks. In some of the older versions of CoAP the proxy is translating the packets without checking whether there is any malicious code injected, this mainly happens when a HTTP client requests resources from a CoAP backend server [7]. Unsecure key management during the initial connection establishment can also lead to MITM attack and loss of secure keys generated for the communication. There are many scenarios where CoAP is under scrutiny due to challenges in terms of security. However, due to many of its features CoAP is more secure and has high provisioning than MQTT, but these are less when compared with HTTP protocol. [11] Gives information on some of the CVEs' found in CoAP.

Mitigations: Most of the mitigations applied to MQTT also applies to CoAP, however due to some extra added features in CoAP, making it more powerful and as its leading in provisioning, there are many security issues which needs to be addressed and mitigated. This survey gives slight instances and concentrates on common mitigation methods to over the problems of MITM attacks. First and foremost important step is to maintain a device in such a way that the attack surface is very less, this is in the hands of manufacturers and developers and their attention towards security in IoT and IIoT devices. Implementing the concept of resource directory in all the devices will ensure that the device is connected to the trusted end-point or known end-points and CoAP supports CoRE (Constrained RESTful Environments) link format, by this we can mitigate and overcome the MITM attacks to a very large extent. Binding DTLS with CoAP ensures that it is safeguarded by SSL and TLS as an encryption layer, and the messages in CoAP transmission are fragmented and encrypted, so that even if an MITM attacker sits in the communication there is a very less chance to decrypt the message though the attacker might get the message, CoAP with DTLS is termed as secure-CoAP [29]. Caching attacks with proxy enabled communication will have ability to gain the control and it pose a threat to the client, unknowing an intruder in the network i.e., MITM attacker, this can also be mitigated by using a secure encryption algorithm and robust key management process provides solutions for many attacks including MITM attacks on CoAP and other protocols. Secure and time-to-time updates on IoT devices from the manufacturers will be a great advantage to mitigate MITM attacks.

Designing IoT devices with secure architecture, preventing unauthorized access to sensors, secure handshake process, and restricting sensitive applications and information access to web can decrease the amount of MITM attacks on IoT devices. [43][44][7][29] Gives a better understanding on how CoAP works, security attacks and analysis in CoAP, transparent interception of CoAP-HTTP, DTLS implementation, milestones completed and what milestones are to be achieved in order to reduce the attack surface on IoT devices embedded with CoAP protocol and those can be somehow related to MITM attacks but

not directly. Following these basic mitigation steps, IoT devices can be protected from MITM attacks in the future

VI. MITM ATTACK METRICS

With the number of IoT devices growing at a rapid pace, due to many light weight and constrained protocols, and many misconfiguration in these devices makes them prone to MITM attacks. This section will slightly touch base on some of the latest metrics related to IoT and IoT security.

As IoT are found everywhere at present, Junniper Research group have estimated that the number of IoT devices and sensors are set to exceed 50 Billion by 2022 and 83 billion by 2024, and the industrial sector using IoT is expected to grow more than 70% by 2024. Due to the Covid-19, the number of IoT devices has significantly grown up in the hospitalization sector. And a developer survey on IoT from Eclipse shows that the security is the top concern for an IoT developer which stands at 39%, and the communication security and Data encryption at rest are two of the widely used techniques for securing IoT in 2020. Out of the deployed communication protocols, HTTP/HTTPS and MQTT are leading with percentages of 51 and 41 respectively, however some devices are built with many other communication protocols including these two and top connectivity is with WiFi at 44%. This shows that most of the communication flowing through WiFi connected devices is at a great risk form MITM attacks. Deployment of software updates and middleware integrations are mostly done through the cloud so that it becomes an easy job for the manufacturers and developers to keep and maintain their devices up to date and free from known vulnerabilities.

Shodan and Statistics: With MQTT being one of the mostly adapted and leading protocols in IoT and is the only protocol becoming more vulnerable to MITM attacks, here are some statistics as per the data collected form Shodan IoT search engine on the number of MQTT servers found on the internet, it turns out that around 43000 MQTT servers are exposed on the internet and approximately 32000 of these servers are with no password protection [28] as shown in the Figure 4. Almost 40% of MQTT servers in the world were found in China and USA, and most of the vulnerabilities represented in in Figure 4 are due to misconfigurations in MQTT servers. Some of the techniques to identify and exploit MQTT vulnerabilities are explained briefly in [28], most of those are also related to MITM attacks.

Shodan and Statistics: With MQTT being one of the mostly adapted and leading

When a python script was created in the purpose of connecting subset of hosts with Shodan to verify if authentication was used. The Return Code form CONNACK packet is used to confirm the connection and it gives the statistics as shown in figure 5 [28]. This is performed on a total of 800 MQTT servers.

This data shows that, nearly 70% of the MQTT servers do not even use authentication and only 11% of them returns as bad username or password in the CONNACK packet [28]. By this we can have an understanding of how prone are these IoT devices to MITM attacks with no or min authentication and encryption, Figure 5 shows authentication results from MQTT server.

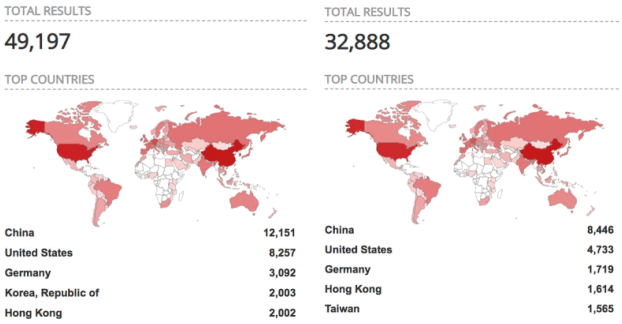

Figure 4: Exposed and Vulnerable MQTT servers on the internet

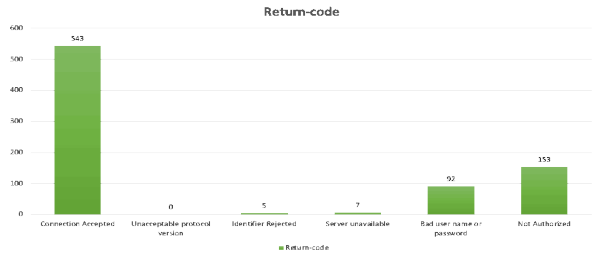

Figure 5: Authentication results from MQTT server

Table 2: Security operations supported by well-known protocols [30]

Protocol	Authentication		Confidentiality		Authorization
	SASL	Custom	TLS	DTLS	Custom
MQTT	No	Yes	Yes	No	No
CoAP	No	No	No	Yes	No
AMQP	Yes	No	Yes	No	NO
XMPP	Yes	No	Yes	Yes	Yes
DDS	No	Yes	Yes	Yes	Yes

Table 2 shows the support of security features like Authentication, Confidentiality and Authorization by well-known and most deployed protocols in IoT devices.

When the analysis on CVEs is made with respect to each and every protocol from year to year, it was found that MQTT took the highest spot in 2019 making it more and more prone to attacks [30], and one of the major attacks was MITM targeting the communication between publishers and subscribers. When representing these CVEs in numbers, MQTT CVE numbers are between 0 to 25 while CoAP CVEs' take up to or in between 30 to 35 and AMQP are high in between 35 to 44 in the year 2019. Similarly in the year 2018, MQTT CVEs' are around 20 while AMQP are around 15 to 35 in numbers with CoAP at 0 in numbers, there are no noticeable CVEs' with CoAP in the year 2018 and before. Some other major protocols high with CVE number are SSDP, XMPP, and mDNS. In the past, although there are very less direct MITM attacks, but DDoS (Distributed Denial of Service) and MITB (Man-In-The-Browser) attacks combined with SSL attacks used to constitute the MITM attacks.

The major IoT protocols became more prone to MITM attacks in the last few years are MQTT, CoAP, XMPP, mDNS, and SSDP. Looking at these huge numbers, one can easily guess how the number of attacks are growing up if there are no proper security measure taken at the time of manufacturing and deployment of these IoT devices.

Due to this huge number of IoT devices and communication among them becoming prone to many attacks including MITM, most of the manufacturers and developers of IoT are now moving towards Edge and cloud computing technology for better security, more reliability of services, minimal management, easy resource shareability, Rapid provisioning and Ubiquitous access. As per the Cisco global cloud index projection, $11/12^{th}$ of work load is done in cloud while $1/12^{th}$ in traditional data center. Even with the help of edge computing, there is a very lower risk for enroute attacks like MITM. [31] Gives very good insights on future of Edge cloud and Edge computing for IoT devices and also discusses many projects which aimed at achieving edge computing with many different kinds of approaches and concepts. Block chain is another technology towards which IoT manufacturers are looking at. As per one of the reports published Gartner, it says 90% of IoT adopters are planning to integrate Blockchain, 39% of these already implemented and 36% of them are planning to implement in the next 12 months. When U.S.A is considered, 75% have already implemented or plan to implement blockchain by the next year. Having blockchain implemented, make these devices very less prone to MITM attacks and other attacks which target on Confidentiality, Authentication and Authorization.

Whatever the technologies and inventions for security are coming up, attackers on the other hand are trying to exploit them and trying to steal sensitive information flowing to/from these devices. The major things to consider for protecting IoT devices from MITM attacks are regular updating of the device software, using SSL certificates, proper firewall configuration in some networks or devices and adaptation to encryption across the system and network.

These are some of the metrics and findings related to IoT devices with a concentration on important protocols which are becoming more prone to MITM attacks.

VII. CONCLUSION

With the pace at which the IoT devices acceptance is growing in the present day-to-day life, they become an important target for the attacker to steal sensitive data and cause huge loss to people, organizations and to the society. Man-In-The-Middle is one of the old, important, and less common attacks happening on IoT devices these days. This survey presents various MITM attack types that could be possible in technologies and protocols involving RFID, BLE, MQTT, HTTP and COAP. As these are some of the major deployments in IoT and IIoT devices in the current world, this survey covers issues, misconfigurations and how manufacturing defects in these protocols can lead to MITM attacks and presents some common and open mitigation techniques along with some metrics to give an understanding of the attack and to overcome problems related to on these protocols.

REFERENCES

[1] Cekerevac, Zoran & Dvorak, Zdenek & Prigoda, L. & Čekerevac, Petar. (2017). INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS. MEST Journal. 5. 15-5. 10.12709/mest.05.05.02.03.

[2] A. Murzaeva, B. Kepçeoğlu and S. Demirci, "Survey of Network Security Issues and Solutions for the IoT," 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2019, pp. 1-6, doi: 10.1109/ISMSIT.2019.8932957.

[3] [JIN14] Jing, Qi, et al. "Security of the Internet of Things: perspectives and challenges."Wireless Networks20.8 (2014): 2481-2501.

[4] G. Rajendran, R. S. Ragul Nivash, P. P. Parthy and S. Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures," 2019 International Carnahan Conference on Security Technology (ICCST), CHENNAI, India, 2019, pp. 1-6, doi: 10.1109/CCST.2019.8888399.

[5] M. Data, "The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table," 2018 International Conference on Sustainable Information Engineering and Technology (SIET), Malang, Indonesia, 2018, pp. 206-210, doi: 10.1109/SIET.2018.8693155.

[6] E. Ahmed, A. Islam, M. Ashraf, A. I. Chowdhury and M. M. Rahman, "Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225283.

[7] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-7, doi: 10.1109/ICBDSC.2016.7460363.

[8] Melamed, Tal. "An Active Man-in-the-Middle Attack on Bluetooth Smart Devices." *International Journal of Safety and Security Engineering* 8.2 (2018): 200-11. *ProQuest.* Web. 1 Nov. 2020. http://dx.doi.org/10.2495/SAFE-V8-N2-200-211

[9] "MITM Attack on MQTT-based IoT using BERT Based Adversarial Message Generation" Henry Wong and Tie Luo. [online] https://aiotworkshop.github.io/published/KDD20-AIoT-camera_ready.pdf

[10]] J. Thomas, S. Cherian, S. Chandran and V. Pavithran, "Man in the Middle Attack Mitigation in LoRaWAN," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 353-358, doi: 10.1109/ICICT48043.2020.9112391.

[11] [online] CoAP Vulnerabilities

[12] T. Salman, Internet of Things Protocols and Standards, 2015.Google Scholar

[13] S. Al-Sarawi, M. Anbar, K. Alieyan and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 685-690, doi: 10.1109/ICITECH.2017.8079928.

[14] Wikipedia:[online] https://en.wikipedia.org/wiki/Bluetooth_Low_Energy

[15] S. Pallavi and V. A. Narayanan, "An Overview of Practical Attacks on BLE Based IOT Devices and Their Security," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 694-698, doi: 10.1109/ICACCS.2019.8728448.

[16] Gomez, Carles; Oller, Joaquim; Paradells, Josep. 2012. "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology." *Sensors* 12, no. 9: 11734-11753. https://www.mdpi.com/1424-8220/12/9/11734

[17] H. Damghani, H. Hosseinian and L. Damghani, "Investigating attacks to improve security and privacy in RFID systems using the security bit method," 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), Tehran, Iran, 2019, pp. 833-838, doi: 10.1109/KBEI.2019.8735043.

[18] [online] https://www.business.com/articles/rfid-for-retail/

[19] R. K and R. C. Hansdah, "Symmetric Key-Based Lightweight Authentication Protocols for RFID Security," 2018 32nd International Conference on Advanced Information Networking and Applications

Workshops (WAINA), Krakow, 2018, pp. 488-495, doi: 10.1109/WAINA.2018.00133.

[20] C. Zhang, W. Zhang and H. Mu, "A mutual authentication security RFID protocol based on time stamp", *2015 First International Conference on Computational Intelligence Theory Systems and Applications (CCITSA)*, pp. 166-170, Dec 2015.

[21] Y. Yinhui and Z. Lei, "Research on a provable security RFID authentication protocol based on hash function", *The Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, pp. 31-37, 2016.

[22] V. Vijaykumar and S. Elango, "Hardware implementation of tag-reader mutual authentication protocol for RFID systems", *Integration the VLSI Journal*, vol. 47, no. 1, pp. 123-129, 2014.

[23] V. Cherneva and J. L. Trahan, "Grouping Proofs for Dynamic Groups of RFID Tags: A Secure and Scalable Protocol," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0097-0103, doi: 10.1109/CCWC47524.2020.9031231.

[24] M. Hosseinzadeh et al., "A New Strong Adversary Model for RFID Authentication Protocols," in IEEE Access, vol. 8, pp. 125029-125045, 2020, doi: 10.1109/ACCESS.2020.3007771.

[25] M. Hosseinzadeh et al., "An Enhanced Authentication Protocol for RFID Systems," in IEEE Access, vol. 8, pp. 126977-126987, 2020, doi: 10.1109/ACCESS.2020.3008230.

[26] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.

[27] [online] mqtt.org and variations and improvements of MQTT from 3.1.1-to-5.0

[28] [online] Avast-security and morphuslabs

[29] S. Raza, D. Trabalza and T. Voigt, "6LoWPAN Compressed DTLS for CoAP," 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, Hangzhou, 2012, pp. 287-289, doi: 10.1109/DCOSS.2012.55.

[30] Nebbione, G.; Calzarossa, M.C. Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet* **2020**, *12*, 55.

[31] Jianli Pan and James McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," IEEE Internet of Things Journal, Special Issue on Fog Computing in IoT, Volume: 5, Issue: 1, pp:439-449, February 2018

[32] Dinculeană, Dan. (2019). Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Applied Sciences. 9. 848. 10.3390/app9050848.

[33] [online] BLURtooth attack and CVE-2020-15802

[34] K. K. Patel, S. M. Patel et al., "Internet of things-iot: definition characteristics architecture enabling technologies application & future challenges", *International journal of engineering science and computing*, vol. 6, no. 5, 2016.

[35] T. Yokotani and Y. Sasaki, "Transfer protocols of tiny data blocks in IoT and their performance evaluation," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 54-57, doi: 10.1109/WF-IoT.2016.7845442.

[36] Gunes Acar, Danny Yuxing Huang, Frank Li, Arvind Narayanan, and Nick Feamster. 2018. Web-based Attacks to Discover and Control Local IoT Devices. In Proceedings of the 2018 Workshop on IoT Security and Privacy (IoT S&P '18). Association for Computing Machinery, New York, NY, USA, 29–35. DOI:https://doi.org/10.1145/3229565.3229568

[37] F. Moldovan, P. Sătmărean and C. Oprișa, "An Analysis of HTTP Attacks on Home IoT Devices," 2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 2020, pp. 1-6, doi: 10.1109/AQTR49680.2020.9129980.

[38] T. Yokotani and Y. Sasaki, "Comparison with HTTP and MQTT on required network resources for IoT," 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, 2016, pp. 1-6, doi: 10.1109/ICCEREC.2016.7814989.

[39] N. Nikolov, "Research of MQTT, CoAP, HTTP and XMPP IoT Communication protocols for Embedded Systems," 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 2020, pp. 1-4, doi: 10.1109/ET50336.2020.9238208.

[40] [online] Hacking-IoT-with-MQTT

[41] [online] Avast Security Blog

[42] Dinculeană, Dan. (2019). Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Applied Sciences. 9. 848. 10.3390/app9050848.

[43] S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 655-660, doi: 10.1109/ICACCS.2019.8728533.

[44] [online] https://datatracker.ietf.org/wg/core/charter/

[45] J. Esquiagola, L. Costa, P. Calcina and M. Zuffo, "Enabling CoAP into the swarm: A transparent interception CoAP-HTTP proxy for the Internet of Things", *2017 global Internet of Things Summit (GIoTS)*, pp. 1-6, 2017.