ISSN No:-2456-2165

Challenges Facing on IoT and Gaps that Exist in the IoT Cybersecurity of Data Transferred by MQTT & CoAP Protocols

Dr. Fatma Abdalla Mabrouk Khiralla
Department of Computer Science, College of Science and Arts in Unaizah, Qussim University, Buraydah, KSA

Abstract:- In the Internet of Things era, data-backed insights are being used by industries and organisations to deliver value. It will provide boundless services to increase productivity and efficiency in the future; however, there are still security issues associated with IoT devices.

This paper discusses IoT security issues and challenges using MQTT and CoAP protocols. As a first step, the cybersecurity hierarchy of the Internet of Things and its infrastructure will be examined. Our next topic will be the Internet of things devices and their weaknesses. There will also be a discussion of the types of protocols on the Internet of Things, for example, HTTP, DDS and XMPP, most of which originated from Internet protocols. In addition to highlighting MQTT and CoAP and comparing them, the study clarifies all previous studies that looked at those protocols. Our final paragraph discussed cybersecurity challenges on the Internet of Things and MQTT and CoAP as the future of IoT.

Keywords:- *MQTT, CoAP, IoT, protocols , cybersecurity , HTTP,DDS ,XMPP*

I. INTRODUCTION

All development of information technology needs Security and Privacy because hacking is common in the digital world. IoT is a new technology in the information technology age, it is connecting digital devices to the Web, and the tally is expanding every day. Digital devices involve a huge of data, which needs Security and Privacy because it can be confidential.

The Mirai attack was made in 2016. It was a powerful attack and had a significant effect later. Dyn, a domain name server (DNS) provider, was attacked by Mirai, so many websites collapsed. It was the most significant DDoS attack. It was hacked by the weak Security of one of the digital devices. Attackers can find one vulnerability in any IoT device and manipulate the whole network's data because IoT devices are closely connected. Appliances which are getting updated after a certain period are more vulnerable. Hackers are not only a threat; one of the major concerns is Privacy. It can also happen that companies that implement IoT devices may sell users' data for the sake of money [20].

Big countries are beginning an effort in privacy provisioning on IoT cybersecurity. The action on a lightweight cryptographic framework, secure routing and forwarding, robustness, and resilience management. Protection is significant in IoT, particularly as the characteristics of such an organisation are diverse. Other than Security for guaranteeing Security within the IoT organisation, lightweight cryptographic primitives are required, suited for the IoT organisation.

In order to preserve privacy, context-aware methods and lightweight conventions are proposed, and most recently, virtualisation methods are utilised to preserve the keenness of the information. However, for lightweight cryptographic primitives, novel solutions are required, which should consume the limited resources of an IoT mote. Apart from that, for example, the SDN arrangement offers to execute lightweight cryptographic arrangements over IoT with the help of centralised directing carried at the SDN controller [22].

II. IOT ARCHITECTURE

IoT architecture can be divided into three layers, the recognition layer, the network layer, and the application layer. The recognition layer, referred to perception layer, is responsible for gathering all kinds of data from the physical world using physical end devices like all sorts of sensors, for example, Global Positioning System (GPS) receivers and thermometers.

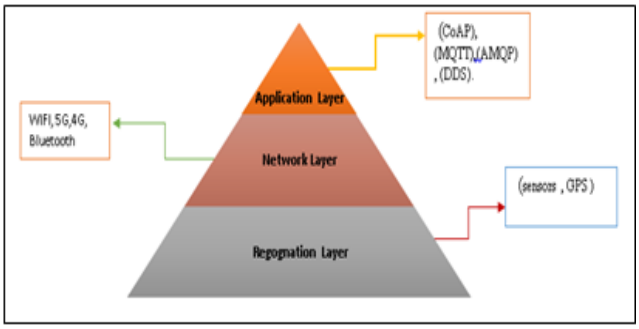

Fig 1:- Architecture of IOT

Network layers have defence types of communication networks like WIFI, 5G, and Bluetooth, which turn on as access networks. Also, it is responsible for the processing and transmission of data. It is an essential layer because it can give

ISSN No:-2456-2165

high-quality services to meet users' needs, show the messaging capability and influence the service's performance. This layer has some protocols such as Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Data Distribution Service (DDS).

With the application layer interface, users can enter the IoT through computers, smartphones, and other devices like the intelligent cooler, smart television, etc., depending on the services. Also can be used the network layer is critical because it serves as the link between the recognition layers and the application layers [17].

III. CYBERSECURITY IN IOT ARCHITECTURE

During a threat modelling exercise, it is recommended to divide a typical IoT architecture into several parts to optimize Security best practices. Devices, Field Gateways, Cloud Gateways, and Services are some of these components.

Each component typically has data and authentication/authorization requirements, so each part can act as a Zone to isolate the damage and limit the impact of low trust zones on higher trust zones.

A Trust Boundary separates each part of data transmitted from one source to another. In this transition, the data could be subjected to spoofing and tampering .FLAUZAC Olivier et al. proposed secure SDN-based architecture for IoT. The proposer works with or without infrastructure. It is based on Software Defined Networking called SDN-Domain. (SDN) emerged as a strategy to increase the functionality of the network, reducing costs, reducing hardware complexity, and enabling innovative research [10]. An infrastructure layer consists below :

- Network devices (e.g., switches, routers, wireless access points).
- Control layer consists of SDN controller(s) (e.g., Floodlight, Beacon, POX, NOX, MUL, Open daylight, etc.).
- An application layer includes the applications configuring the SDN (e.g., Access control, traffic/security monitoring, energy-efficient networking, and network management) [10].

The authors presented a new architecture with multiple SDN controllers in equal interaction. A critical feature of SDN architecture is its ability to extend the security perimeter to the network access endpoint devices by setting up security policy rules for network devices. Furthermore, via the OpenFlow protocol, the SDN controller builds a global network view by establishing a connection with the OpenFlow switches [10].

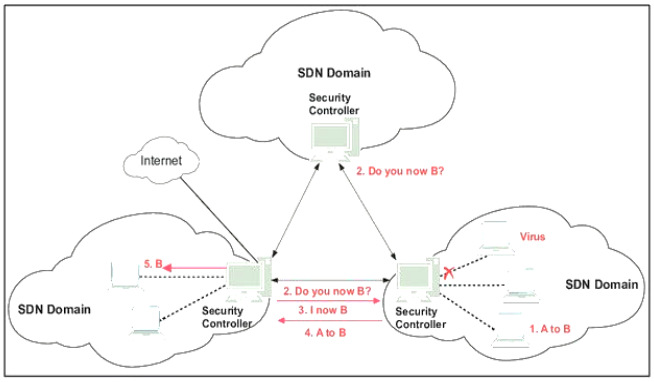

Fig 2:- Security in SDN Domain[10]

IV. THE TYPE OF DEVICES IN IOT

IoT devices come in a variety of types. However, some of them are more visible than others. IoT devices are almost any electronic device with a network connection or has an embedded IoT device.

1. **Devices that gather info and then transmit :**Sensors do the gathering task. Many types of sensors are available like temperature, motion, moisture, and sensors to check air quality, light, etc. These sensors can automatically gather information from their surrounding area or environment and transmit it to the system to which it is connected.
2. **Devices get info, then process and react:** Any device must have a system to which it is connected. This device gathers information and transmits it as received by the system.
3. **Devices doing both jobs :**It can be the system that performs both tasks of gathering and transmitting information to the system and processing it and taking action according to the processed report [20].

V. THE WEAKNESS OF IOT DEVICES

The general idea of IoT is things, especially everyday objects, that are readable, recognisable, locatable, and addressable through information sensing devices or control devices via the Internet, irrespective of the communication, whether via RFID, wireless LAN, or wide area networks. Objects include not only the electronic devices we encounter or the products of higher technological development, such as vehicles and equipment, but things we do not ordinarily think of as electronic. Such as food, clothing, chair, animal, tree, water, etc. The number of devices is increasing day by day [15].

Today IoT and its application to several domains have global relevance, such as industrial automation, intelligent energy management, automotive applications, and healthcare. Although, these diverse applications use many things like sensors, actuators, and devices to communicate via the Internet. The heterogeneous nature often leads to a waste of resources and inefficiency.

The Lack of a unified approach to handling heterogeneous devices from several vendors presents a significant challenge in IoT device management [4]. A study published in July 2020 analysed over 5 million IoT, IoMT (Internet of Medical Things), unmanaged connected devices in healthcare, retail, manufacturing, and life sciences. It reveals numerous vulnerabilities and risks across a stunningly diverse set of related objects. They include shadow IoT (devices in active use without IT's knowledge), compliance violations, and US Food and Drug Administration recalled (defective and risky) medical devices. The report shows facts below:

15%	of smart devices were anonymous or unauthorized.
19%	were uses unsupported operating systems.
49%	of IT teams were guessing IT solutions to get vision.
59%	were unaware of what kind of smart devices were active in their network.
75%	of deployments had VLAN violations
86%	of medical care, deployments have more than ten FDA rejected devices.
95%	of medical care networks integrated Amazon Alexa and Echo devices beside hospital monitors tools.

Table 1:- Statistic to study a vulnerabilities and risks across Iot devices[15]

VI. INSECURE INTERFACES ON IOT

The web interface is the part of control through which the user can interact. IoT devices today to communicate with the Internet and have some kind of web interface. In an innovative hospital, for example, the internet router web interface is accessible using a default IP defined by the user or a doctor. In numerous cases, control and arrangement may be required when talking approximately IoT. Considering the ease of executing a web interface for gadgets that are associated to the net, it's secure to accept that most IoT gadgets will be and as of now are utilising an interface of the sort[25].

IP-based IoT and IPv4 (Internet Protocol version 4) hackers attacked the fourth version of the Internet Protocol (IP). IP-based IoT and IPv4are core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. These attacks are black-hole attacks, spoofing, smurfing, and eavesdropping. So means IoT requires the same security measures as required for IPv4 because it is imagined with IoT that the physical world will be associated with the Web, which leads to a wide assortment of security concerns. Attack dangers not as it were incorporate control of data but real control of gadgets in IoT networks. With more electronic systems, i.e., Modbus and SCADA becoming part of IP-based systems, a significant increase in attacks is expected.

On the other hand, in a wireless mobile network, a remote portable organisation, a course is built up when course data is transmitted from hub to hub until the goal is found.. This route is maintained daily, and phase nodes are added or deleted.

During this route setup and discovery phase, several attacks are possible by malicious nodes in routing table overflow attack by transmitting a considerable amount of false route information to neighbouring nodes, which cause the neighbour's routing table to overflow. Due to such actions, the table is filled with spurious routes, and fundamental ways are denied from occupying the routing table [22].

VII. IMPORTANT PROTOCOLS ON IOT

The Internet of Things (IoT) is one of the essential topics in academia and Cybersecurity. As IoT frameworks are heterogeneous, supporting more than one protocol may be an option. In addition, a combination of scaling-down-hardware manufacturing, micro-computing, and machine-to-machine (M2M) communication has enabled IoT advancements. According to Gartner. Billions of dollars are being spent on IoT-enabling innovations, and much more is expected in the coming years.

IoT protocols include Constrained Application Protocol (CoAP), Advanced Message Queuing Protocol (AMQP), Digital Data Service (DDS), Message Queue Telemetry Transport (MQTT), and Hypertext Transfer Protocol (HTTP). Several of these protocols are new, while others are derived from a previous version.

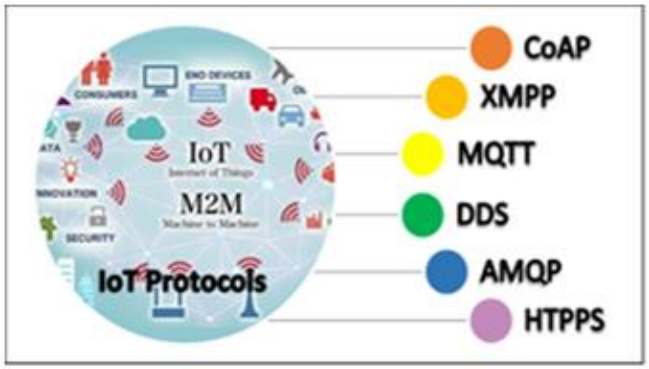

Fig 3:- Protocol architectures for IoT domains

Technologies in the IoT enable non-computer objects to interact intelligently and take collaborative decisions that can be useful for specific applications. For example, permitting things to listen, see, think, or act allows them to communicate with others and create choices that can be as basic as saving lives or buildings.

They change "things" from passively computing and making individual choices to effectively and ubiquitously communicating and collaborating to form a single fundamental choice. IoT depends on ubiquitous computing, embedded sensors, light communication, and web protocols to succeed, but they also present challenges and the requirements for technical measures and communication protocols.

A. Hypertext Transfer Protocol (HTTP)

The HTTP protocol is an application-level, bland, stateless protocol that is used to communicate information over the World Wide Web. One of the critical features of HTTP is the substance arrangement of the information representation. It enables various heterogeneous gadgets to be built autonomously from the information to be shared. HTTP

may be a request-response protocol where the client sends an ask message, and the host responds with a response message. HTTP adaptation 3.0 (H3) is the most recent version of HTTP introduced in 2018. However, HTTP 1.1 is still the most commonly used today [9].

B. Constrained Application Protocol (CoAP)

The Internet of Things (IoT) must reduce control utilisation to coordinate entire frameworks on a small chip. Low prices will enable IoT devices to be found in homes, factories, [16] and other environments. A CoAP is a web utility protocol for compelled devices. It is designed to connect IoT devices through driven systems that have low bandwidth availability. It is customised to meet the requirements of low-cost devices and IoT application scenarios.

By sending a CoAP packet, a client can command another node. The CoAP server will interpret it, extract the payload, and decide what to do based on its logic. The server does not need to acknowledge the request.[23].

The CoAP protocol is generally used for machine-to-machine communication (M2M) and is particularly suited for IoT frameworks based on HTTP protocols. For lightweight communication, CoAP utilises the UDP protocol. It moreover employments restful engineering, which is similar to the HTTP protocol. Finally, it uses a compact parallel architecture based on UDP (or DTLS if Security is enabled), which allows communication through multicast.

URIs address the CoAP assets, and Web Media Types represent resource states. In addition, serene caching and proxying enable arrangement flexibility. Nevertheless, CoAP offers features beyond HTTP 1.1, making it more suitable for IoT.

C. Data Distribution Service (DDS)

DDS IoT protocols have two fundamental layers: Data-Centric, Publish-Subscribe (DCPS), and Data Local, Reconstruction Layer (DLRL) [9].DLRL allows the sharing of distributed information among IoT-enabled objects by exposing an interface to DCPS functionalities, and DCPS is in charge of exchanging the truths with supporters.[26] In contrast to MQTT and CoAP protocols, DDS implements a broker-less architecture. It uses multicasting to provide the applications with high-quality QoS. The DDS protocol can be transmitted from low-impression devices to the cloud [15].

D. The Message Queue Telemetry Transport (MQTT) Protocol

MQTT, developed by IBM and currently an OASIS standard,, stands for Message Queuing Telemetry Transport and is an open message protocol defined by OASIS. In a central server, messages are sent to endorsers based on topics (like kitchen/oven/temperature) that clients can subscribe to. One of the main focuses is on minimising code and minimising network bandwidth [11].

The MQTT protocol facilitates one-to-many communication through brokers. Messages can be published to brokers by clients, and/or subscribers can subscribe to brokers to receive notifications. The topics act as "labels" for arranging messages for mailing to subscribers [23]. Scalability is one of the critical advantages of the MQTT protocol. This protocol supports many small, constrained devices, providing a simple way to ensure asynchronous communication between them [6].

Additionally, MQTT has disadvantages; it is not recommended for IoT applications due to the need for TCP support. TCP increases reliability but has issues with mobility and Security. So, MQTT considers SSL/TLS secure and data encrypted [6]. Another disadvantage of MQTT compared to AMQP is that it offers few control options, and real-time communication happens in seconds. In contrast, AMQP has been designed for speed, not reliability[6].

E. Extensible Messaging and Presence Protocol (XMPP)

The Extensible Messaging and Presence Protocol (XMPP) is an open-source protocol for building real-time applications. it contains a wide range of service communication capabilities such as instant messaging, multi-party chat, voice and video calls, collaboration, lightweight middleware, and centralised distribution of XML information [8].

As part of the central determination, XMPP provides built-in point-to-point encryption (TLS). However, because XMPP uses XML, which is text-based, this results in a higher overhead compared to similar encoding protocols, such as CoAP, MQTT, AMQP, and DDS. Furthermore, XMPP uses open-ended XML streams over TCP and supports small XML data units called XML stanzas [8].

An XMPP cluster is made up of multiple servers within a single domain. Through clustering, XMPP systems can be interoperable. For example, figure 16 illustrates how an innovative house system is built using XMPP [9].

VIII. COMPARISON BETWEEN MQTT & COAP

Using Secure Technology is one challenge in Cybersecurity. IoT devices and protocols can be generally problematic in the Internet environment.

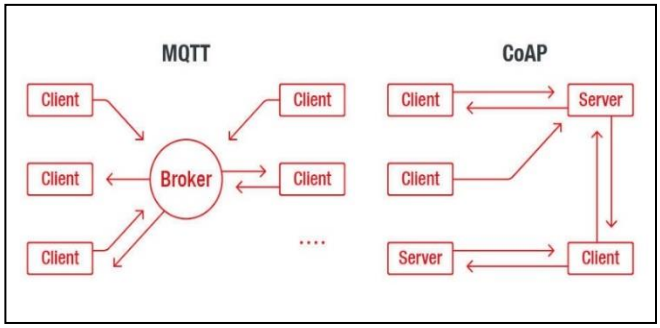

Fig 4:- A high-level view of the interaction models of MQTT (left) and CoAP (right)

ISSN No:-2456-2165

In mission-critical communications, MQTT is preferred to CoAP because it enforces quality of service and ensures message delivery. In addition, the CoAP protocol is selected for gathering telemetry data transmitted from transient, low-power nodes, such as tiny field sensors. In IoT and IIoT deployments, both protocols are fundamental to providing fast and flexible data exchange, which is a crucial operational requirement.

Hundreds of thousands of MQTT and CoAP hosts can be reached via public-facing IP addresses. As a result, attackers have access to millions of records. Furthermore, due to the inherent openness of protocols and the public availability of deployments, it is possible to locate exposed endpoints in virtually every country.

Trend Micro also found examples of hackers attacking protocols IOActive's Lucas According to Lundgren, over 65,000 IoT servers on the Internet that use the Message Queuing Telemetry Transport (MQTT) protocol do not use authentication or encryption. Also, he developed a tool that could be used to attack MQTT-based servers, see the data being sent and received, and control the devices.

Lundgren presented at Black Hat USA 2017 and detailed the potential for taking over the world through MQTT and stated that he could view the coordinates of aeroplanes, electrical meter readouts, and the status of home automation and alarm systems. Additionally, he was able to issue firmware updates, send messages, and open prison doors [12].

A study was conducted concerning the performance of CoAP and MQTT[24]. According to the survey, MQTT introduces TCP overhead, which makes it more bandwidth demanding. Additionally, it has different QoS and implicitly provides reliability, while CoAP only offers a simple mechanism for QoS and reliability through confirmable or non-confirmable messages. Securing communications with DTLS or TLS (CoAP) significantly increases bandwidth usage – more than 1000% in CoAP and 74 to slightly over 200% in MQTT – as well as CPU usage – about 3.5% for PSK and 11.5% for PKI in CoAP and about 27% for PSK and 36% for PKI in MQTT – taking into account the modes of operation and QoS. Secure communications are also adversely affected by latency losses more than lossless networks.

MQTT	CoAP
Using MQTT, devices can communicate over a wide area network (WAN, internet).	Its compatibility with HTTP is its strongest use case
If bandwidth is limited, MQTT is most useful.	If an IoT developer wants to leverage an existing web server architecture, then CoAP is the way to go.
Because of its established architecture, it can easily be adapted to current development needs.	The CoAP protocol designed for resource-restricted environments.

Table 2:- compering between MQTT protocol & CoAP protocol

IX. PREVIOUS STUDIES ON COMPARING COAP AND MQTT

CoAP and MQTT have been compared in small-scale trials over an unnamed radio technology[5]. In addition, a healthcare use case was implemented with prototype hardware in[5]. This study demonstrates how 5G massive IoT can be realised over an NB-IoT network. Furthermore, simulation results confirm the hypothesis that MQTT, a TCP-based system, adversely affects both device perceived throughput, system load, and service availability and coverage.

MQTT and CoAP have been compared in[18], where they are both used on smartphones. According to the study by Niccolò De Caro et al. [], CoAP can be a valid alternative to MQTT in specific scenarios. Both protocols can meet the needs of smartphone-based crowdsensing applications in terms of performance and functionality.

The two protocols were compared and discussed in detail in the study, qualitatively and quantitatively. According to the qualitative comparison, MQTT is more appropriate for applications requiring advanced functionalities, such as message persistence, wills, and "once-and-for-all" delivery. Moreover, CoAP can only support unicast communications, making MQTT the best solution when secure multicast is a priority.

CoAP is also showing better results both in terms of bandwidth usage and round-trip time, according to the preliminary performance analysis. Therefore, CoAP makes an appropriate choice when aiming to reduce network and device resource usage through its caching feature. As a result, smartphone radio connectivity is less demanding and presents fewer challenges than NB-IoT in terms of throughput, availability, coverage, and battery life [2].

A simulation study was conducted to confirm the working hypothesis that MQTT, as a TCP-based system, negatively impacts the device's perceived throughput and the system load, as well as service availability and coverage. CoAP confirms a lightweight and low-cost alternative to TCP when a sensor report is approved. According to a study Anna .

Larmo et al. [2]. The study confirms that MQTT, a TCP-based system,, negatively impacts the device's perceived throughput, system load, and service availability and coverage. A lightweight and inexpensive alternative to TCP is CoAP confirm, which confirms sensor report transmission.

X. IOT CYBERSECURITY CHALLENGES

Although The Internet of Things (IoT) opens up incredible opportunities for industries to connect "things" and change how they operate, market and serve their customers with greater insight, however, there have been many projects that have shortcomings in some IoT projects.

ISSN No:-2456-2165

A leading technology Beecham Research and research, an analysis firm specialising in IoT, undertook an extensive study into the subject, consisting of both primary and secondary research, including a survey of 25,000 IoT adopters. The results show that Nearly three-fifths (58%) of businesses said that their IoT projects had been unsuccessful—just 12% said they'd been entirely successful [14].

Security is a common concern for all new technologies. And IoT is no exception. There have been many horror stories about IoT devices which were being hacked. However, this isn't indicative of any particular weakness of the IoT but relatively poor product development and management processes.

The main goals of IoT security are to ensure all data is collected, stored, processed, and transferred securely to Detect and eliminate vulnerabilities in IoT components. Original website apriorit.com [1], a list of common security challenges with the Internet of Things as shown below:

A. Vulnerability:

Ensuring the Security of IoT systems is very tricky Many IoT systems have security vulnerabilities for many reasons, Lack of computational capacity for efficient built-in Protection, Poor access control in IoT systems, Limited budget for adequately testing and updates due to limited budgets, and technical limitations of IoT devices Users may not update their devices.Poor Protection from physical attacks: attackers can get close enough to add their chip or hack the device using radio waves.

B. Insecure communications:

One of the most dangerous threats caused by insecure communications is the possibility of a man-in-the-middle (MitM) attack. Hackers can efficiently perform MitM assaults to compromise an overhaul strategy and take control of your gadget on the off chance that it doesn't utilise secure encryption and confirmation components. Aggressors can indeed introduce malware or alter a device's usefulness. Indeed in case, your gadget doesn't drop casualty to a MitM assault, the information it trades with other gadgets and frameworks can still be captured by cybercriminals on the off chance that it sends it in cleartext messages. Associated gadgets are vulnerable to assaults from other gadgets. For occurrence, attackers can easily compromise all other unisolated devices if they gain access to just one device in a home network.

C. Malware dangers:

A later think about by Zscaler found that gadgets most at the hazard of being hacked by malware were set-top boxes, smart TVs, and smartwatches. A few organisations have, as of now, found ways to bargain with the foremost popular IoT-targeted malware. For occurrence, an FBI operator shared how the office halted the Mirai botnet assaults, and Microsoft has discharged a direct on how to proactively protect your frameworks against the Mozi IoT botnet. But unfortunately, hackers keep inventing new ways to abuse IoT networks and devices. For example, in 2021, researchers discovered that BotenaGo, malware written in Golang, can exploit more than 30 vulnerabilities in smart devices.

D. Cyberattacks:

Denial-of-service (DoS) attacks commonly occur on IoT devices. Denial-of-service attacks are highly susceptible to IoT devices because of their limited processing power. A DoS attack affects a device's ability to handle legitimate requests by flooding it with fake traffic.

XI. THE FUTURE OF MQTT AND COAP

In recent years, the Internet of Things has been used more widely, allowing new ways for devices to be connected. IoT transactions require protocols to ensure efficiency and efficient traffic management.

IoT protocols are the backbone of its systems; MQTT, HTTP and CoAP are prevalent protocols (Figure 8). MQTT as a standard is presented in [6]. MQTT is a lightweight protocol that uses a subscriber/publisher model with high efficiency suitable for the IoT environment of low-powered constrained devices[6] .

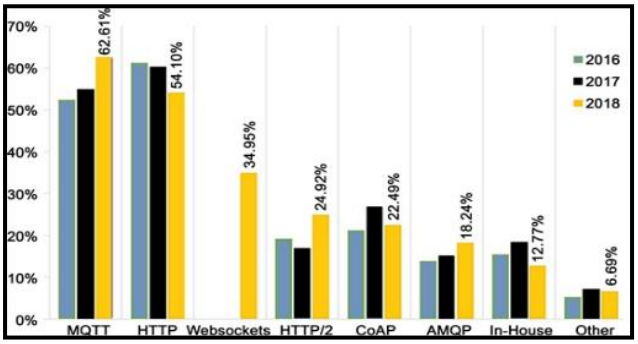

Fig 8:- 2016-2018: comparison Changes in Usage of Protocols in IoT environments [6].

MQTT is gaining significant popularity - the big cloud providers have jumped on board or did so initially. Moreover, MQTT offers valuable features for many commercial applications.

Some applications standardised around HTTP (such as mobile apps) may opt to utilise CoAP both for peripherals and back-end communication to reduce bandwidth usage when connecting to faulty networks [13].

According to a study by Daniel Silva et al. that compared the performance of the two protocols when comparing the size of the messages versus the frequency of the messages, both protocols exhibit similar performance, even though CoAP shows a spike when messages are less frequent (IAT of 1000 ms).

The repeated experiments resulted in significantly higher TTC(stands for trying-to-conceive), suggesting that the CoAP setup mechanism impacts TTC significantly. MQTT and CoAP protocols can be used effectively in many applications throughout the Internet of things.

In their study, Ashar Tariq et al. [3] discuss the open research challenges in CoAP implementation related to Security, interoperability, resource discovery, energy efficiency, and congestion control.

In a study, the authors suggested that the current architecture of CoAP may become inefficient as the number of internet devices keeps growing. The highlighted research gaps give insight into future research directions for improving CoAP performance in dense network scenarios.

XII. CONCLUSION

The Internet of Things faces significant challenges when it comes to expanding securely. Security is the essential aspect of the Internet of Things, specifically the protocols through which data is transmitted because many vulnerabilities make hacking data easier. In this paper, we have reviewed the performance of the CoAP and MQTT protocols because the CoAP protocol and MQTT protocol are essential protocols for the Internet of Things. As a result of their lightness, they can also meet most of the functional and performance requirements of collective sensing applications based on smartphones. The reliability and congestion control mechanisms of MQTT are the most complex. CoAP is suitable for developing efficient applications to reduce network and device resource usage. There are some limitations in the data transmission process with CoAP and MQTT. Due to its TCP overhead, MQTT requires more bandwidth, whereas CoAP simply provides a simple mechanism for QoS and reliability.

REFERENCES

[1]. Anna Katrenko, Elena Semeniak,feb/2022, https://www.apriorit.com/dev-blog/513-iot-security
[2]. Anna Larmo et al,2018**, Impact of CoAP and MQTT on NB-IoT System Performance**, Journals Sensors, https://www.mdpi.com/journal/sensors
[3]. Ashar Tariq et al.,2020, **Enhancements and Challenges in CoAP—A Survey**, Sensors 2020.pp.1-29
[4]. Biliyaminu Umar et al, 2018,**Evaluation of IoT Device Management Tools**, The Third International Conference on Advances in Computation, Communications and Services,pp.15-21
[5]. Chen, Y., Kunz, 2016, **Performance evaluation of IoT protocols under a constrained wireless access network**, International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT), Cairo, Egypt, April 2016,pp. 1–7
[6]. Daniel Silva et al,2021, **A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA**, MDPI Journals,pp.1-30
[7]. DDS Protocol Architecture basics | DDS Protocol in IoT, *https://www.rfwireless-world.com/Terminology/DDS-protocol-architecture.html)*
[8]. *Extensible Messaging and Presence Protocol (XMPP). Apr. 18, 2020.[Online]. Available: https://xmpp.org*
[9]. EYHAB AL-Masri et al,2020, **Investigating Messaging Protocols for the Internet of Things**, IEEE open access, VOLUME 8,pp. 94880- 94911
[10]. FLAUZAC Olivier. el al,2015, **New Security Architecture for IoT Network**, Procedia Computer Science, SENACYT-Panama, Secretar´ıa Nacional de Ciencia, Tecnolog´ıa e Innovaci´on,pp. 1028 – 1033
[11]. Georg Aures, Christian Lübben,2019, **Network Architectures and Services**,pp.1-5
[12]. *https://www.blackhat.com/us-17/briefings.html on 15/8)*
[13]. Jonathan Fries, 2017, **Why are IoT developers confused by MQTT and CoAP**, /www.techtarget.com/iotagenda/ ,Why are IoT developers confused by MQTT and CoAP? - IoT Agenda (techtarget.com)
[14]. Jürgen Krämer,2021, **Why IoT projects fail and how to beat the odds**, https://www.idglat.com/afiliacion/whitepapers/2020-5-ar-why-iot-projects-fail-en.pdf?tk=/:
[15]. Keyur K Patel.el al,2016, **Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges**, International Journal of Engineering Science and Computing, Volume 6 Issue No. 5,pp.6122-6131
[16]. Matthias Kovatsch et al,2014, **Scalable Cloud Services for the Internet of Things with CoAP**, IEEE
[17]. Musa G. Samaila.el al.2018, **Challenges of securing Internet of Things devices**: A survey, Fundação para a Ciência e a Tecnologia ,Volume1, Issue2,pp.1-32
[18]. Niccolò De Caro, el al ,2013, **Comparison of two lightweight protocols for smartphone-based sensing**,EEE 20th Symposium on communications and Vehicular Technology in the Benelux (SCVT), pp. 1–6.
[19]. OMG Data Distribution Service (DDS) Version 1.4 book available on https://www.omg.org/spec/DDS/1.4
[20]. Ravi Kumar.el al.,2020, **Literature Review of IoT & 5G**, International Journal of Engineering Research & Technology (IJERT) Volume 8, Issue 05,pp.1-5
[21]. S.Profanter, A. Tekat, K. Dorofeev, M. Rickert, and A. Knoll,"**OPC UA versus ROS, DDS, and MQTT: Performance evaluation of industry 4.0 protocols,**" in Proceedings of the IEEE International Conference on Industrial Technology (ICIT), Feb. 2019. [Online]. Available: http://mediatum.ub.tum.de/doc/1470362/1470362.pdf
[22]. Sufian Hameed.el al.,2019, **Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review**, Journal of Computer Networks and Communication, Volume 2019, pp.1-14
[23]. TREND MICRO RESEARCH ,2018,MQTT and CoAP: Security and Privacy Issues in IoT and IIoT Communication Protocols - Noticias de seguridad - Trend Micro ES,access on 15/8/2021
[24]. Victor Seoane et al ,2021, **Performance evaluation of CoAP and MQTT with security support for IoT environments**, Elsevier journals Computer Networks Volume 197,pp.1-22

[25]. web interface, **OWASP Top 10 for IoT** – Explained, Available: https://checkmarx.com/wp-content/uploads/2015/07/OWASP_TOP_10_IoT_Explained.pdf
[26]. https://www.rfwireless-world.com/Terminology/DDS-protocol-architecture.html