International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 4, April-2022, Impact Factor: 7.957

Messaging Protocols for the Internet of Things

Prashant Verma

Master of Science in Computer Science, Georgia Institute of Technology, Atlanta, Georgia, USA
MBA, Haas School of Business, University of California Berkeley, California, USA.

ABSTRACT

The present study consists in carrying out a systematic review of the use of the different messaging protocols that are used by the Internet of Things (IoT). Intelligent environment management, healthcare, industrial, home automation, and smart cities are just some of the many examples of how IoT can improve our lives. One of the challenges for IoT development is the growing number and heterogeneity of devices. Because of the wide range of technologies utilized in the IoT, middleware and development frameworks with well-defined abstractions are required. An inadequate protocol can affect the key aspects of performance and obsolescence. The messaging protocols presented in the study support the interaction between applications, devices, and services in the request-response, publish-subscribe with the transmission variations over UDP and TCP, etc. The discussion involves the various types of messaging protocols available for IoT with their own unique features to let the readers decide the direction to follow as the next step for experimentation with the presented protocols. Finally, this research serves as a guide for future researchers and developers involved in projects based on IoT products in a way that supports them in choosing the appropriate messaging protocols in an objective and reliable manner.

Keywords:Internet of Things, IoT, Smart Devices, Smart Technology, Messaging Protocols, CoAP, HTTP, MQTT, WebSocket, AQMP, XMPP, DDS, Application Protocol, Communication Protocol.

1. INTRODUCTION

Over the years, the worldwide computer network and the Internet have been confused as synonymous with one of its most important applications: the World Wide Web, or just the Web. While the Internet itself is an infrastructure that allows the inter-connecting hundreds of thousands of computers, the Web is a fantastic repository of information and of human knowledge, which has evolved over the years. Initially, it was called Web 1.0, in which the focus was the search and delivery of information to people (i.e., information was made available by a few individuals and accessed by a significantly larger number of users). In Web 2.0, people go from being consumers of information to also the producers of information. The focus became collaboration and sharing of information, where the main phenomenon is the creation and dissemination of different social networks. In this evolutionary line, the next step is Web 3.0, also called Semantic Web [1], characteristic in a simplified way by obtaining and automated information processing. One different way of analyzing this evolution is through the Internet itself, which has gone from a network that connected computers to be seen as a document repository and subsequently a network of the interconnection of people and now, more recently mind of objects, or things more precisely called the Internet of Things (IoT) [2]. Many of the devices that traditionally do not connect to the Internet are beginning to be developed and manufactured with Internet connection availability interacting both person-to-machine (P2M) and machine-to-machine (M2M) to coordinate activities in order to fulfill the same purpose.

IoT is a paradigm that aims to create a connection anytime, anywhere, for everything with low capacity and processing power in different application areas such as personal and social communication, business, and service monitoring [3]. As a result of intensive research in the field of IoT in recent years, many limited or extensive new devices and sensors have been produced [4]. Present estimates suggest that the number of IoT devices will exceed 30 billion by 2023, with more than 200 billion intermittent connections, creating a market of over $700 billion [1], [5], [6]. Many factors need to be considered in data transmission. Depending on these factors, different communication models and protocols with different usage scenarios have been created. CoAP, HTTP, MQTT, WebSocket, AMQP, XMPP, and DDS are some of the popular protocols used in data transmission in IoT.

The main objective of this research is to carry out a systematic review of the different messaging protocols for the IoT which are currently in use. The result of this study serves as a guide for product developers so that it can help them choose the appropriate protocol that can interact and operate within a globalized environment.

2. IoT MESSAGING PROTOCOLS

Internet protocols are a fundamental part of the connectivity of IoT devices, and it is logical to contemplate how devices are going to connect for communication [7]. The representation of communication models that connect and communicate directly with each other and not through servers. However, to establish communications between the devices, there are some protocols that need to be surveyed. In the following sub-sections, a review and introduction of these protocols have been presented.

A. CoAP – Constrained Application Protocol

CoAP is a software protocol that has also been designed to be used in electronic devices. This protocol is designed to be used in small low-power devices in order to move the HTTP protocol, including other requirements such as multicast, low overhead and simplicity. This protocol is semantically aligned with the HTTP protocol which allows easy mapping of the two protocols [8]. The managed condition of the protocol for network devices is restricted with smaller microcontrollers and amount of flash memory while in local networks. Figure 1 shows the architectural framework of CoAP working.

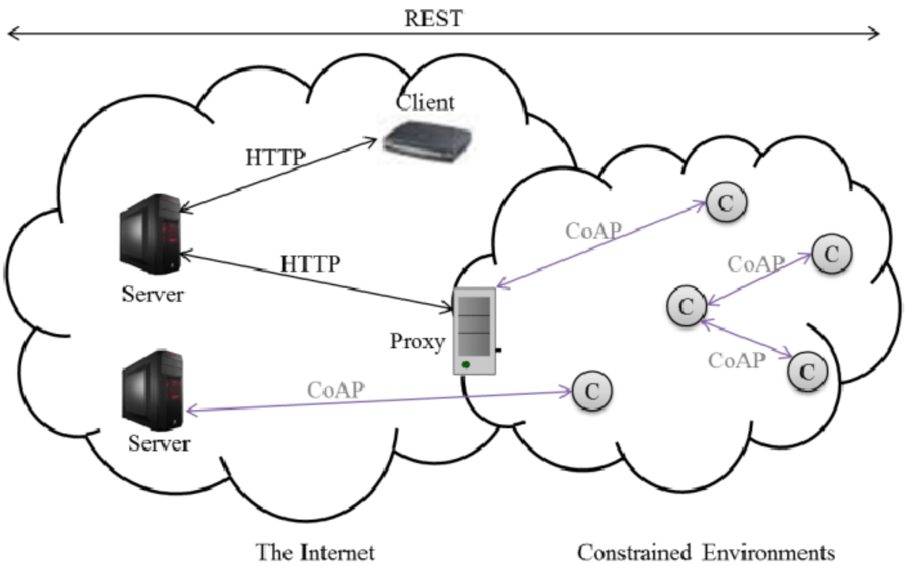

Figure 1. Working of CoAP Protocol

CoAP is suitable for devices that operate with a battery or use energy extraction. This is one of the protocols used in the industry and in the transfer of documents. The CoAP protocol is based on REST and has been referenced in IoT since it is coupled to the client/server model, which is evolving the applications, being convenient for IoT scenarios [9].

B. HTTP – Hypertext Transfer Protocol

HTTP is a well-known protocol in the industry and is the basis of the client/server model used for the Web [8], [10]. It is also considered one of the most vulnerable protocols in IoT devices. It can be made more secure if the device can initiate connections to a Web server but is barred from receiving connection requests [11]. This protocol provides transport but does not define the presentation of the information, so when making a request, it can contain HTML, JSON, JavaScript, and XML, among others [12]. On the other hand, this information transmission standard is used to establish a communication medium so that a computer that requests information communicates with a server through the Web and can interoperate or communicate in the same protocol. This is where the protocol influences IoT devices, seeking that the technology they use can communicate quickly and securely [13]. For this reason, the HTTP protocol shows the fundamental need for IoT technology to safely interconnect devices that have been created for their correct operation.

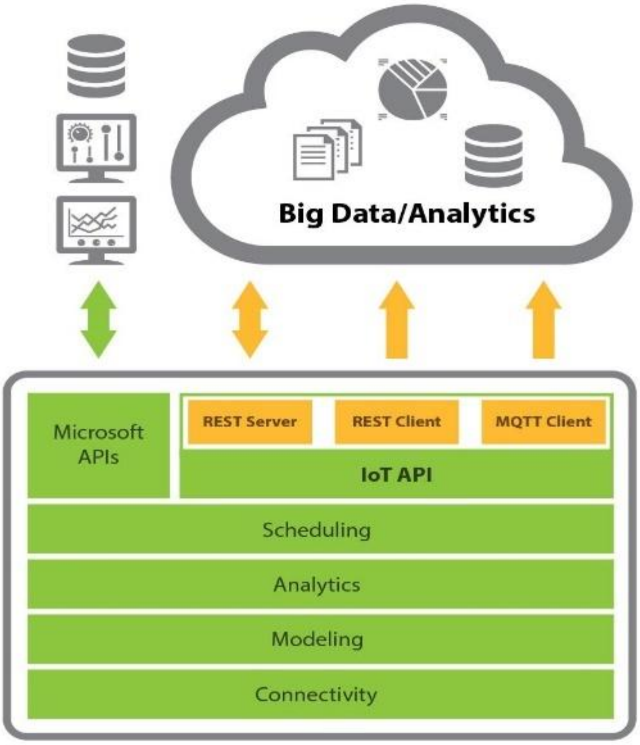

Figure 2. Working of HTTP with IoT API

Figure 2 shows us the client/server REST model. HTTP has limitations in its use since it is effective when sending text or document information, but when sending videos, the speed is slow. The Internet is a complicated network of information exchange between computers that are separated by a great distance; these types of digital technologies are critical in laying the foundations for information order and transmission [14]. HTTP is a protocol for communicating between a client's requests and a server's answers via the Internet. TCP/IP is utilized in IoT devices to implement this protocol, which is one of the earliest.

C. MQTT – Message Queuing Telemetry Transport Protocol

This is one of the publish/subscribe service protocols. The infrastructure is used by clients that connect to a central server called a broker. Publisher, subscriber, and server are the three essential components of MQTT [15]. The publisher is the originator of the created data, and its goal is to convey it to the subscriber. Message and Topic are the two essential components of data. Subscribers are the target users who receive it to analyze and process the disseminated data. Figure 3 below shows a schematic of the protocol.

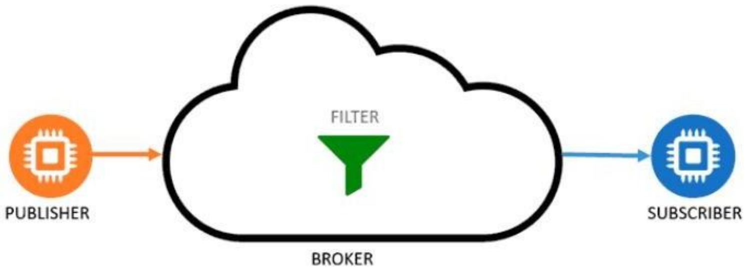

Figure 3. Working of MQTT

MQTT is designed for remote networks. Like HTTP, its payload is specific to the application, implementing the custom or binary JSON format [15], [16]. This protocol is not used widely as HTTP but has an industry share of the ICT market. IoT devices support both MQTT and HTTP as the primary input protocols. MQTT is generally preferred in IoT applications due to its low energy consumption and bandwidth requirement, high scalability, and very small header size [15]. However, MQTT requires a TCP/IP connection that offers sequential and lossless connection capability [17]. This structure is quite complex for small, simple, and affordable sensor-based devices. To address this issue, MQTT-SN for wireless networks was developed. MQTT-SN can be considered as an alternative to MQTT that has the characteristics of the wireless communication environment [18]. Unlike MQTT in the MQTT-SN system, IoT objects are connected via a wireless connection to a gateway / intermediary device using an MQTT-SN protocol. This gateway device is connected to the broker over a wired connection using the MQTT protocol. Another difference is that the MQTT-SN protocol communicates over UDP. UDP is more suitable for sensor applications as it brings faster, simpler, and lighter code load than TCP in wireless connections [19].

D. AMQP – Advanced Message Queuing Protocol

AMQP is another subscribe and publish based protocol. It was initially developed for the financial services sector, but now it has a limited presence in ICT as well. The main function of this protocol is to cover reliability and interoperability [20]. It is also used as an a-synchronicity complement with HTTP. Figure 4 below shows how it works.

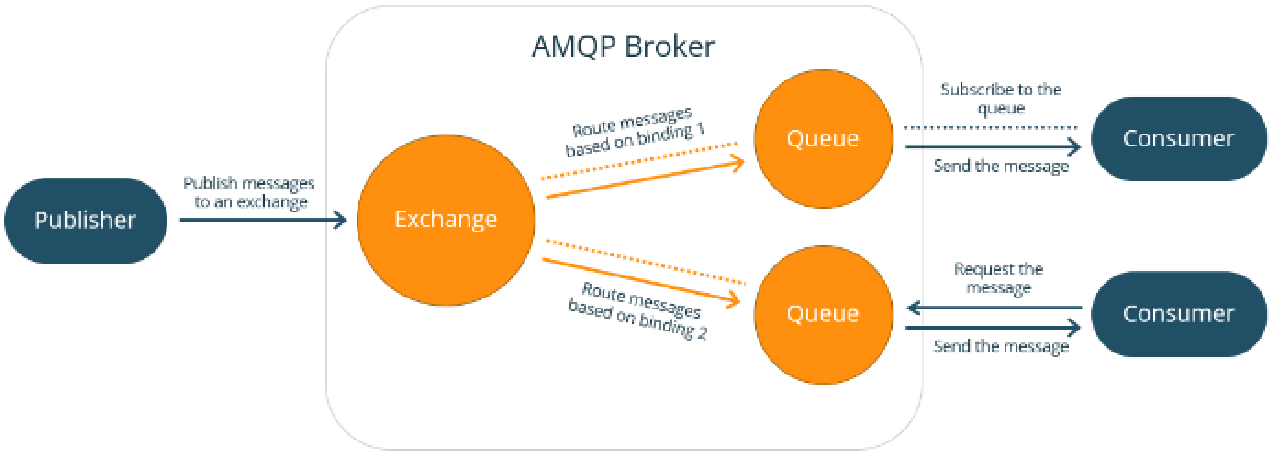

Figure 4. Working of AMQP

AMQP is an intermediation protocol with queuing capacity, and this protocol is aimed at sending messages with security and reliability characteristics. However, this type of protocol is not scalable. The biggest benefit of this protocol is its robust communication model, which guarantees complete transactions and is useful in IoT technology. It is used in applications such as autonomous computing, cloud computing, and even in IoT security aspects [21].

E. WebSocket Protocol

The WebSocket protocol was created to allow clients and servers to communicate in real time. A WebSocket connection is established by HTTP requests and includes a handshake [22]. Following that, the messages are sent through TCP. It is supposed to replace present bidirectional technological tools that take advantage of existing infrastructure by using HTTP as a transport layer. Figure 5 below shows this working principle.

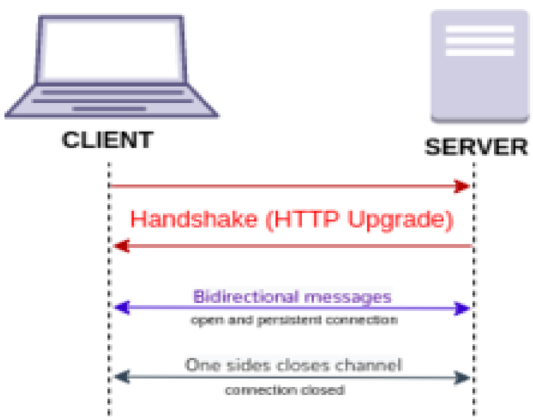

Figure 5. Working of WebSocket

Both parties can send messages to each other at any moment, even simultaneously, as long as the connection is open. WebSocket connections can be made without encryption, like with HTTP or with TLS encryption. As a result, the WebSocket protocol is suitable for transferringhuge amounts of data, as well as streaming. Unless the handshake closes the connection between these two ends, it stays open.

F. XMPP - Extensible Messaging and Presence Protocol

XMPP is an instant messaging protocol developed by the Internet Engineering Task Force (IETF) that may be used in numerous sessions, audio and video chats, and teleconferences [23]. The Jabber open-source community created it to provide an open-source, secure, spam-proof, and stand-alone communications system. XMPP allows users to connect with one another via the Internet by exchanging instant messages, independent of the operating system they are using. In Figure 6 below, a general XMPP communication is schematized where gateways can bridge different messaging networks.

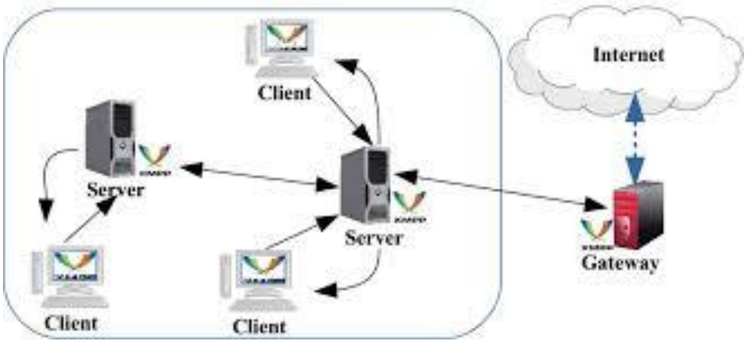

Figure 6. Working of XMPP

Many instant messaging apps assessed within the realm of IoT have selected XMPP due to its various characteristics. Its autonomous structure allows it to function on a variety of internet-based platforms. It is safe and enables the development of new apps on top of the kernel structure. An XML stanza stream connects the client and server in XMPP. An XML stanza is a section of code that is separated into three pieces. Message, presence, and iq (information/query) are the three components [24]. The source and destination addresses, kinds, and IDs of XMPP entities that conduct the push technique to obtain the data are specified in message stanzas. The title and text of the message are filled in the subject and body areas by the message stanza.

G. DDS - Data Distribution Service

The Object Management Group created DDS, a protocol for real-time machine-to-machine (M2M) communication.Unlike other publish/subscribe communication protocols like MQTT and AMQP, DDS is built without the use of a broker [25]. In addition, it uses multicastingto provide the best QoS (Quality of Service) structure and high stability in its applications. Figure 7 below represents the workflow of DDS.

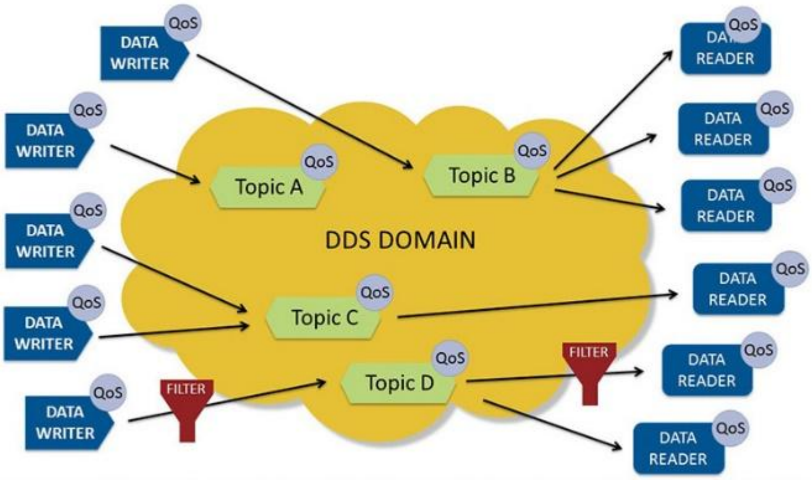

Figure 7. Working of DDS

Data Centric Publish-Subscribe (Data Centric Publish/Subscribe - DCPS) and Data-Local Reconstruction Layer are the two levels defined by the DDS architecture (DLRL). DCPS is in charge of disseminating information to subscribers. DLRL, on the other hand, is a DCPS function interface with an optional usage. It makes it easier for public data to be shared among disparate objects[26].

Data transit is permitted within the DDS domain, a virtual environment of the networked publisher and subscriber apps. In DCPS, there are five entities that can be stated in the data flow. These are: (1) the publisher who distributes the data, and (2) the data writer who interacts with the publisher regarding the data content and changes based on the type. The data writer and publisher connection imply that the application will publish relevant data with the content given; (3) the subscriber receiving the broadcast data, (4) the data reader used to retrieve the received data, and (5) the header (Topic) which creates the relationship between the data reader and writer.

3. COMPERATIVE REVIEW OF IoT MESSAGING PROTOCOLS

In the previous section, the general definition, architectural structures and message transmission models of several communication protocols that are frequently used in IoT are discussed. In this section, the mentioned protocols are compared over different features.

Application developers on the Internet of Things are concerned about device limits, bandwidth constraints, and energy usage. The decision of the messaging protocol to be utilized to send or receive data is an essential issue that must be handled. To date, all such protocols have originated and developed to fulfil a variety of demands. Messaging protocols also differ in some ways from one another due to differences in needs and techniques for meeting those needs. Table 1 summarizes some features of messaging protocols discussed in this study.

TABLE 1. COMPERATIVE REVIEW OF IoT MESSAGING PROTOCOLS

Feature	CoAP	HTTP	MQTT	AMQP	WebSocket	XMPP	DDS
Transmission Protocol	UDP	TCP	TCP	TCP	TCP	TCP	TCP or UDP
Architecture	Client → Server	Client → Server	Client → Tool → Subscriber	Client → Tool → Subscriber, Client → Server	Client → Server	Client → Server → Subscriber	Client → Subscriber
Transmission Model	Request → Response	Request → Response	Publisher → Subscriber	Publisher → Subscriber	Request → Response and Later Stream	Publisher → Subscriber	Publisher → Subscriber
Minimum Header Size	4 Bytes	-	2 Bytes	8 Bytes	16 Bytes	-	-
Security	DTLS, SSL	SSL	TLS / SSL	TLS / SSL, IP-Sec, SASL	TLS / SSL	TLS	SSL, DTLS
XML Support	No	Yes	No	No	Yes	Yes	No
QoS Support	Yes	No	Yes	Yes	Yes	No	Yes
Default Port	5683/5684	80/443	1883/8883	5671/5672	80/443	80/443	7400/7401
Interoperability	Semantic	Semantic	Foundational	Structural	Semantic	Structural	Semantic
Governed By	IETF	IETF, W3C	OASIS	OASIS	IETF	IETF	OMG

4. CONCLUSION

In this study, messaging protocols that are frequently used in IoT are discussed by considering their working logic and architectural structures. The researcher discussed the renowned and widely used messaging protocols namely CoAP, HTTP, MQTT, AMQP, WebSocket, XMPP and DDS. Each of these has its own unique features and working conditions to support IoT devices. It is very difficult to give preference or rank any one of these as all of these have their own pros and cos to implement for diverse range of IoT applications. The contexts of development and applications on which the IoT will have an exponential growth, given the immense number of devices that are taken to the networkdepends largely on allowing interoperability between various providers that offer these technologies.The approach of descriptive research should be extended to larger studies and research approaches of most of the messaging protocols referenced here.For this reason, the present investigation applies an approach towards a systematic review with an analytical and descriptive analysis of these protocols for the home and industry. The IoT is a revolution in constant development and progress.Thereare still many challenges to cover to achieve its implementation. This work focused on the systematic review and analysis of messaging protocols for IoT however it is recommended to approach the review from different scenarios that still require study such as reliability, security, availability and reliability etc. due to continuous and significant changes un underlying technology.

REFERENCES

[1] T. Berners-Lee, R. Fielding, and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” *www.rfc-editor.org*, Jan. 2005, doi: 10.17487/RFC3986.

[2] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The internet society (ISOC),* vol. 80, pp. 1-50, 2015.

[3] M. Hung, "Leading the iot, gartner insights on how to lead in a connected world," *Gartner Research,* vol. 1, pp. 1-5, 2017.

[4] A. Chaudhary, S. K. Peddoju, and K. Kadarla, "Study of internet-of-things messaging protocols used for exchanging data with external sources," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2017: IEEE, pp. 666-671.

[5] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013.

[6] O. Mazhelis *et al.*, "Internet-of-things market, value networks, and business models: State of the art report," *University of Jyvaskyla, Department of Computer Science and Information systems, Technical Reports TR-39,* 2013.

[7] K. Rose, S. Eldridge, and L. Chapin, "The Internet of things: An overview. Internet Society,(October), 53," ed, 2015.

[8] D. Rathod and S. Patil, "Security analysis of constrained application protocol (CoAP): IoT protocol," *International Journal of Advanced Studies in Computers, Science and Engineering,* vol. 6, no. 8, p. 37, 2017.

[9] S. Cirani, G. Ferrari, M. Mancin, and M. Picone, "Virtual replication of iot hubs in the cloud: A flexible approach to smart object management," *Journal of Sensor and Actuator Networks*, vol. 7, no. 2, p. 16, 2018.

[10] D. Priyadarshi and A. Behura, "Analysis of different iot protocols for heterogeneous devices and cloud platform," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018: IEEE, pp. 0868-0872.

[11] O. Bello, S. Zeadally, and M. Badra, "Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)," *Ad Hoc Networks,* vol. 57, pp. 52-62, 2017.

[12] J. Tournier, F. Lesueur, F. Le Mouël, L. Guyon, and H. Ben-Hassine, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet of Things,* vol. 16, p. 100264, 2021.

[13] B. Yong, X. Liu, Q. Yu, L. Huang, and Q. Zhou, "Malicious Web traffic detection for Internet of Things environments," *Computers & Electrical Engineering,* vol. 77, pp. 260-272, 2019.

[14] F. Pereira and L. Gomes, "A JSON/HTTP communication protocol to support the development of distributed cyber-physical systems," in *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, 2018: IEEE, pp. 23-30.

[15] G. P. Naik and A. U. Bapat, "A Brief Comparative Analysis on Application Layer Protocols of Internet of Things: MQTT, CoAP, AMQP and HTTP," 2020.

[16] J. Sidna, B. Amine, N. Abdallah, and H. El Alami, "Analysis and evaluation of communication Protocols for IoT Applications," in *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications*, 2020, pp. 1-6.

[17] P. Gupta, "A Survey of Application Layer Protocols for Internet of Things," in *2021 International Conference on Communication information and Computing Technology (ICCICT)*, 2021: IEEE, pp. 1-6.

[18] K. Govindan and A. P. Azad, "End-to-end service assurance in IoT MQTT-SN," in *2015 12th Annual IEEE consumer communications and networking conference (CCNC)*, 2015: IEEE, pp. 290-296.

[19] S. P. Jaikar and K. R. Iyer, "A survey of messaging protocols for IOT systems," *International Journal of Advanced in Management, Technology and Engineering Sciences,* vol. 8, no. 2, pp. 510-514, 2018.

[20] G. Caiza, E. S. Llamuca, C. A. Garcia, F. Gallardo-Cardenas, D. Lanas, and M. V. Garcia, "Industrial shop-floor integration based on AMQP protocol in an IoT environment," in *2019 IEEE Fourth Ecuador Technical Chapters Meeting (ETCM)*, 2019: IEEE, pp. 1-6.
[21] E. Al-Masri *et al.*, "Investigating messaging protocols for the Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 94880-94911, 2020.
[22] G. M. Oliveira *et al.*, "Comparison between MQTT and WebSocket protocols for Iot applications using ESP8266," in *2018 Workshop on Metrology for Industry 4.0 and IoT*, 2018: IEEE, pp. 236-241.
[23] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
[24] A. Singh, A. Payal, and S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," *Journal of Network and Computer Applications*, vol. 143, pp. 111-151, 2019.
[25] S. A. Laghari, S. Manickam, and S. Karuppayah, "A review on SECS/GEM: A machine-to-machine (M2M) communication protocol for industry 4.0," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 10, no. 2, pp. 105-114, 2021.
[26] N. M. Elzein, M. A. Majid, I. A. T. Hashem, I. Yaqoob, F. A. Alaba, and M. Imran, "Managing big RDF data in clouds: Challenges, opportunities, and solutions," *Sustainable Cities and Society*, vol. 39, pp. 375-386, 2018.