ISSN 2289-6376 DIGES PMU 8 (2021) 212–218

Review on Smart Agriculture: Internet of Things (IoT) Application Layer Protocols

Amir Haziq Loh Bojeng[1,*], Nurhazura Hassan[2], and Rozaida Halil[3]
[1]Examination Unit, Politeknik Mukah, KM 7.5, Jalan Oya, 96400 Mukah, Sarawak, Malaysia
[2]Industrial Relations and Training Unit, Politeknik Mukah, KM 7.5, Jalan Oya, 96400 Mukah, Sarawak, Malaysia
[3]Department of Information Technology and Communication, Politeknik Mukah, KM 7.5, Jalan Oya, 96400 Mukah, Sarawak, Malaysia
*Corresponding author: amir.haziq@pmu.edu.my

Abstract

The Internet of Things (IoT) is one of computing field that currently growth and hottest trend for any related field in current years. The IoT is a concept where it enables every "thing" or device to connect, communicate and make a decision for the application in many fields including healthcare, disaster recovery, home automation, automation vehicle, Agriculture and etc. During the last century, the basic agriculture technology likes machines has been used. Nowadays, the modern technology adoption for the agriculture improvement. Though the modern technology, the farmers able to do a better job or are slightly improved from their predecessors. This paper review on the previous works that are related to the IoT protocols and this review is to identify the possible IoT protocol that could be used to develop an IoT System for agriculture. This review also focusing on the protocol that could working in a constrained environment. From the finding, Message Queue Telemetry Protocols (MQTT) are suitable to be used in a constrain environment (low communication bandwidth and unstable connection) and be able to operate in high latency environment, lightweight, and the most importance is reliable to be used in the smart agriculture applications.

Keywords: - *Internet of Things (IoT), IoT protocols, smart farming, smart agriculture*

1. Introduction

An Internet of Things (IoT) is a concept where a group of "things" or devices are connected to each other, communicate through the network or internet and the devices operate with less human interactions (Aazam et al., 2018). In other word it operates intelligently. With the existing of IoT, human daily life is made easier and more efficient due to the enabling of devices to become more intelligence and easy to access by the users (Triantafillou et al., 2018). From time to time the number of IoT devices are growth rapidly. Base on the prediction by Cisco IBSG, the number of IoT devices will reach 50 billion by 2020 (Evans, 2011). In 2017, Gartner predicted that, by 2020 IoT devices will increase to 20.4 billion units (Gartner, 2017). In the last past decades, the communication network is only be used in computers and mobile phones applications. However, in recent years, the communications networks have been used to connect home appliances, vehicle, parking system, sensors and many more. Indirectly it shows that the IoT devices are widely develop and use.

Due to the existence of IoT in agriculture, it brought the great revolution in this industry. By advancement of technologies now a day, the agriculture industries are able to find the solution to manage the resources and productivity issues (Farooq et al., 2019). However, in some case, the agriculture areas are having an issue on the unstable connectivity. Some developer developed a system without considering a suitable protocol because those protocol doesn't matter as long as the system could run in developer's environment (which is the connectivity is not an issue). At the end, during the deployment stage, the system could not run properly. There for, choosing a suitable protocol in developing an agriculture system are importance. In choosing the right protocol, a few considerations should be taken into account including energy efficiency, performance, resources usage, and reliability. In this paper, a few types of applications layers protocols have been reviewed and a suggestion protocol to be use for developing a system that suitable in constrained agriculture areas has been made.

2. IoT Application Layer Protocols for Constrained Agriculture System

There are few architectures has been provided for the IoT. However, IoT architecture generally represented as a multiple set of layers as shown in Figure 1 (Luzuriaga et al., 2015).

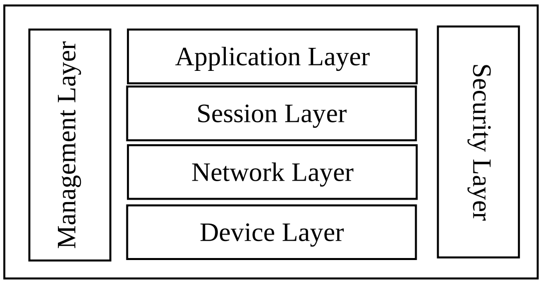

Figure 1: IoT Architecture. (Luzuriaga, et al., 2015)

This reference architecture consists of four layers including device layer, network layer, session layer and application layer. Each of this layer has their own protocols used. However, this paper only focusing on the application layer protocols of Internet of Things. According to (Andy et al., 2017), Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (C0AP), Advance Message Queuing Protocol and Message Queue Telemetry Protocols (MQTT) are most common use protocols in IoT Application layer. Those protocols have a lightweight message overhead, a small message size, and has a message management property (Andy et al., 2017).

2.1 Message Queue Telemetry Protocols (MQTT)

MQTT was first introduce by Andy Stanford Clark back in 1990. In 2013, it was standardized by OASIS. It runs over TCP/IP (Salman and Jain, 2017). According to Lombardi et al. 2021, MQTT is a protocol that supports the network with low bandwidth and high latency. Luzuriaga et al. 2015 also mention that MQTT protocol has solved the problem thar arise due to the unstable communication. This protocol is among the lightweight protocols that work on publish-subscribe model (Soni and Makwana, 2017). Besides, it is a simple and easy to deploy protocol which make this protocol suitable to be use in a constraint environment (Mishra and Kertész, 2020). In MQTT, there are 4 main component which is a broker, a topic, a publisher and a subscriber (Dobbelaere et al., 2017). Figure 2 shows the message Exchange model in IoT for MQTT protocol.

In this exchange model, a device could be a publisher where it can publish a message or a subscriber to receive the message from the topic it interested to or both (Jasenka et al., 2018). A broker is a centre component which is equivalent to a server. It acts as a centre node to enable the publisher to publish or send a data or to enable subscriber to receive a data with the help of a topic. (Sonawala et al., 2017).

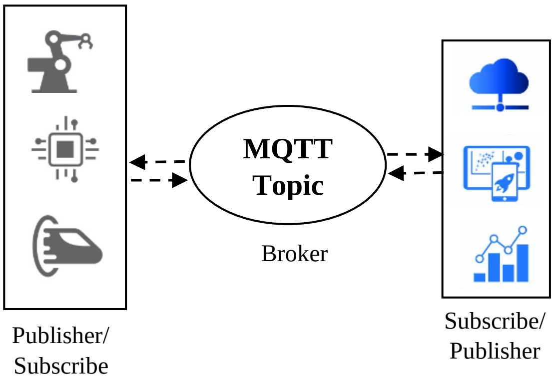

Figure 2: Message exchange model in IoT for MQTT protocol

2.2 Constrained Application Protocol (CoAP)

CoAP was introduced by Internet Engineering Task Force (IETF) and Constrained RESTful Environment working group known as CORE for providing lightweight RESTful interface (Mishra and Kertész, 2020). This protocol is similar to the HTTP concept which handling the communication with 3 a way handshaking. However, CoAP is build over UDP Platform. This is to reduce the overhead of this protocol. Once the overhead has been reduced, the reliability of this protocol also been reduced too. Figure 3 shows the architecture of CaAP (Mishra and Kertész, 2020).

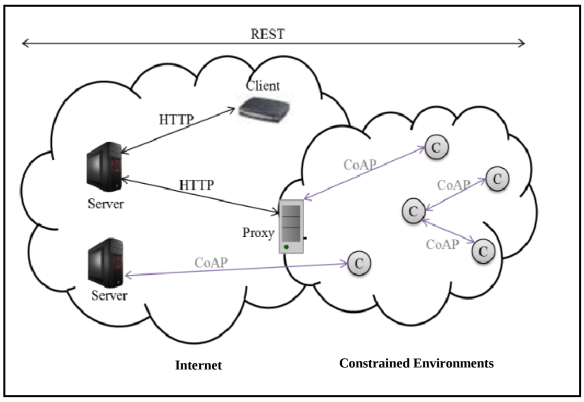

Figure 3: CoAP architecture

In this protocol architecture, it is divided into 2 sub layer which is message layer and request/response layer. Message layer are responsible to manage the redundancy and the consistency of message while the communication handled by request/ response layer.

There are four (4) transmission mode for CoAP which are Confirmable Mode, Non-Confirmable mode, Piggyback mode and Separate mode. Figure 4 illustrate 4 message transmission mode for CoAP (Salman and Jain, 2017).

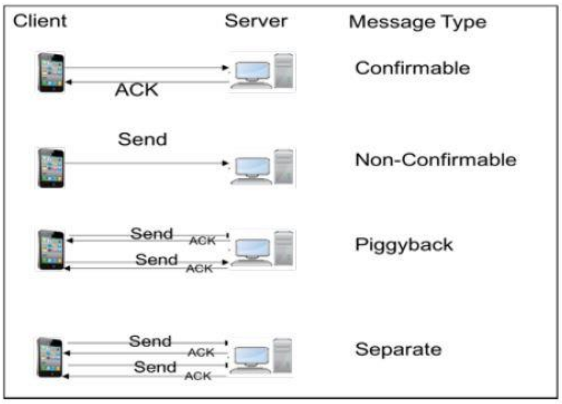

Figure 4: CoAP message transmission mode

Based on the Figure 4, the confirmable mode represents the reliable transmission mode where the message send with this mode will send repeatedly until the acknowledgement received by the sender. Non-confirmable mode represents a non-reliable transmission mode where no acknowledgment will be received by the sender. Piggyback is a mode used for client/server direct communication. The sender will receive an acknowledgment once received confirmable message or non-confirmable message. While the separate mode is a method to stop the sender send the message repeatedly by sending an empty message instate of sending an acknowledgment (Ansari et al., 2018).

2.3 Advanced Message Queuing Protocols (AMQP)

Beside the MQTT, another protocol that has been standardized by OASIS are Advanced Message Queuing Protocol (AMQP) and was designed to be use in financial industry and business management. Similar to MQTT, AMQP is using publish/subscribe model (Salman and Jain, 2017). Based on Köksal and Tekinerdogan (2017), this protocol is a server-to-server protocol where it sends the transactional messages between servers. Figure 5 shows the communication model of AMQP.

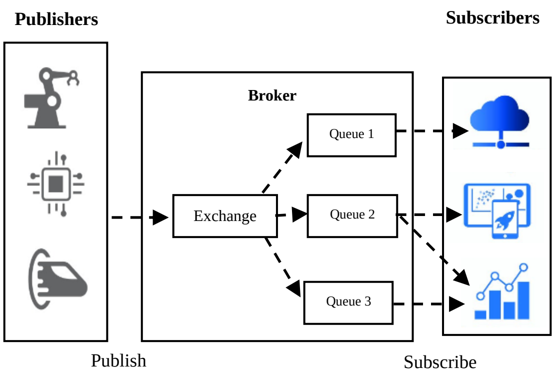

Figure 5: Communication model for AMQP

The AMQP communication is almost the same as MQTT since it used the same publish/subscribe model. The only difference between AMQP and MQTT communication model is in AMQP, the Broker are divided into 2 component which are Exchange and Queue. Exchange is responsible to receive the message that was published by the publisher and distribute it to the queue based on predefined rules. Once the data are available in the queue or known as topic, the subscriber that has connected to the Queue/ topic will get the data that has been published by the publisher (Köksal and Tekinerdogan, 2017). AMQP has an interoperability feature where it allows the system with difference languages and platform to exchange message (Dizdarevic et al., 2018). Besides, it can support any size of message and enable this protocol to handle the exchange of large number of messages (Luzuriaga et al., 2014).

2.4 Hyper Text Transfer Protocol (HTTP)

HTTP is a protocol that commonly in communication protocol and the oldest protocol used in IoT (Grigorik, 2013). This protocol was standardize based on IETF standard. It is a client/server model protocol and using request/respond format of messaging. In order to do create, read, update and delete (CRUD) operations, GET, POST, PUT and DELETE methods are used in this protocol. HTTP running on TCP/IP protocol model and using 3-way handshake communication proses. Due to that, it required high resources and less suitable running with the environment with low power (Dizdarevic et al., 2018 and Banks and Gupta, 2014).

3. Performance Analysis and Comparation on IoT's Application Layer Protocols Used in IoT

From the review on the works that has been carry out by other researcher related to the commonly used protocol in IoT, the performance analysis of various Application layer protocols has been carried out based on different criteria including architecture, Header size, message size, overhead, power consumption, resource requirement, latency, bandwidth, IoT usage, QoS and reliability. Table 1 shows the comparison of MQTT, CoAP, AMQP and HTTP that commonly used in IoT environment. This protocol has been study, proposed and implemented and has been analyzed by other researcher in different applications and areas (Sonawala et al., 2017; OASIS, 2012; Luzuriaga et al., 2014; Naik, 2017; (Dobbelaere et al., 2017; Bormann et al., 2018 and Saint-Andre, 2004). The outcome from those researchers is, HTTP is a protocol that has a good scalability however it is not reliable. CoAP is a simple protocol and consume low CPU and memory resource however on the other hand, CoAP has a high latency, bad packet delivery and unable to be used for complex data type (Yassein et al., 2016). AMQP is a protocol that is highly scalable and could operate the system with difference platform and language. It also has an ability to support industrial environment. However, AMQP are not suitable to handle an application that is in the constrained environment (Al-Fuqaha et al., 2015). While MQTT is a lightweight machine to machine (M2M) communication protocol. It provides the resources efficiency for the information exchange. Its support the communications with low bandwidth and high latency. Indirectly it could solve the problem that arise with unreliable communications (Luzuriaga et al., 2015). Table 1 shows the comparison between MQTT, CoAP, AMQP and HTTP.

Table 1: Comparison of IoT application layer.

Criteria	MQTT	CoAP	AMQP	HTTP
Year	1999	2010	2003	1997
Architecture	Client/Broker	Client/Server or Client/Broker	Client/Broker or Client Server	Client/Server
Abstraction	Publish/Subscribe	Request/Response or Publish/Subscribe	Request/Response or Publish/Subscribe	Request/Response
Transportation Protocol	TCP	UDP	TCP	TCP
Header Size	2 Bytes	4 Bytes	8 Bytes	Undefined
Message Size	Small and Undefined (upto 256MB maximum size) Higher then CoAP	Small and undefined (Small to fit in single IP datagram) Lower then MQTT	Negotiable and Undefined Higher then MQTT but lower than HTTP	Large and Undefined Highers among all protocol
Message Overhead	Medium (Higher than CoAP)	Low	Medium (Higher then MQTT and Lower than HTTP)	High
Power Consumption	Medium (Higher than CoAP)	Low	Medium (Higher then MQTT and Lower than HTTP)	High
Resource Requirement	Medium (Higher than CoAP)	Low	Medium (Higher then MQTT and Lower than HTTP)	High
Latency	Medium (Higher than CoAP)	Low	Medium (Higher then MQTT and Lower than HTTP)	High
Bandwidth	Medium (Higher than CoAP)	Low	Medium (Higher then MQTT and Lower than HTTP)	High
Reliability	High	Medium (Higher than HTTP and Lower than AMQP)	Medium (Higher then CoAP and Lower then MQTT)	Low
QoS	High	Medium (Higher than HTTP and Lower than AMQP)	Medium (Higher then CoAP and Lower then MQTT)	Low
Standards	OASIS, Eclipse Foundation	IETF, Eclipse Foundation	OASIS, Eclipse Foundation	IETF and W3C
IoT Usage	High	Medium (Higher to HTTP but Lower to AMQP	Medium (Higher to CoAP but Lower to MQTT)	Low

4. Conclusion

This paper is reviewing previous works that is related to the commonly used IoT protocols and focusing on the Application Layer protocols IoT enable Smart Agriculture environments. From this review, a discussion and comparison between the protocols has been made based on those protocol criteria and performances. Each of those protocol has their own advantage and disadvantages based on the application. However, in this paper, the main focus is to evaluate which protocol is suitable for the agriculture field with the constrained environment. In the constrain environment, the most important criteria to be taken into account are resource and power consumption, tolerance to the latency and also the network communication requirements. Based on the finding, Message Queue Telemetry Protocols (MQTT) is the most suitable layer protocol to be used in the constrained environment due to it criteria which is light wight, low power consumption, low latency and reliable.

References

Aazam, M., Zeadally, S., & Harras, K. A. (2018). Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Transactions on Industrial Informatics*, *14*(10), 4674-4682.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

Alkuhlani, A. M. I., & Thora, S. B. (2015). Internet of Things (IoT) Standard Security Issues. *In International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 491-495.

Andy, S., Rahardjo, B., & Hanindhito, B. (2017, September). Attack scenarios and security analysis of MQTT communication protocol in IoT system. In *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* (pp. 1-6). IEEE.

Ansari, D. B., Rehman, A., & Ali, R. (2018). Internet of things (iot) protocols: a brief exploration of mqtt and coap. *International Journal of Computer Applications*, *975*, 8887.

Banks, A., & Gupta, R. (2014). MQTT Version 3.1.1. *OASIS standard*.

Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., & Raymor, B. (2018). CoAP (Constrained Application Protocol over TCP, TLS and Websockets RFC8323. *RFC Editor*.

Deshmukh, S., & Sonavane, S. S. (2017, March). Security protocols for Internet of Things: A survey. In *2017 International conference on Nextgen electronic technologies: Silicon to software (ICNETS2)* (pp. 71-74). IEEE.

Dizdarević, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. *ACM Computing Surveys (CSUR)*, *51*(6), 1-29.

Dobbelaere, P., & Esmaili, K. S. (2017, June). Kafka versus RabbitMQ: A comparative study of two industry reference publish/subscribe implementations: Industry Paper. In *Proceedings of the 11th ACM international conference on distributed and event-based systems* (pp. 227-238).

Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016, September). A survey on secure communication protocols for IoT systems. In *2016 International Workshop on Secure Internet of Things (SIoT)* (pp. 47-62). IEEE.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11.

Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access*, *7*, 156237-156271.

Gartner. (2017). Gartner . Retrieved September 2, 2021, from http://www.gartner.com/newsroom/id/3598917.

Goossens, M., Mittelbach, F., & Samarin, A. (2013). *CAN System Engineering: From Theory to Practical Applications*. Springer International Publishing A G.

Grigorik, I. (2013). Making the web faster with HTTP 2.0. *Communications of the ACM*, *56*(12), 42-49.

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 ieee world congress on services* (pp. 21-28). IEEE.

Hwang, H. C., Park, J., & Shon, J. G. (2016). Design and implementation of a reliable message transmission system based on MQTT protocol in IoT. *Wireless Personal Communications*, *91*(4), 1765-1777.

Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of things Journal*, *1*(3), 265-275.

Kianmajd, P., Rowe, J., & Levitt, K. (2016, April). Privacy-preserving coordination for smart communities. In *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1045-1046). IEEE.

Köksal, Ö., & Tekinerdogan, B. (2017, June). Feature-driven domain analysis of session layer protocols of internet of things. In *2017 IEEE International Congress on Internet of Things (ICIOT)* (pp. 105-112). IEEE.

Kraijak, S., & Tuwanut, P. (2015, October). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In *2015 IEEE 16th International Conference on Communication Technology (ICCT)* (pp. 26-31). IEEE.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

Lee, S., Kim, H., Hong, D. K., & Ju, H. (2013, January). Correlation analysis of MQTT loss and delay according to QoS level. In *The International Conference on Information Networking 2013 (ICOIN)* (pp. 714-717). IEEE.

Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information*, *12*(2), 87.

Luzuriaga, J. E., Perez, M., Boronat, P., Cano, J. C., Calafate, C., & Manzoni, P. (2015, January). A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)* (pp. 931-936). IEEE.

Luzuriaga, J. E., Perez, M., Boronat, P., Cano, J. C., Calafate, C., & Manzoni, P. (2014, September). Testing AMQP protocol on unstable and mobile networks. In *International Conference on Internet and Distributed Computing Systems* (pp. 250-260). Springer, Cham.

McEwen, A., & Cassimally, H. (2013). *Designing the internet of things*. John Wiley & Sons.

Mishra, B., & Kertesz, A. (2020). The use of MQTT in M2M and IoT systems: A survey. *IEEE Access*, *8*, 201071-201086.

Mun, D. H., Le Dinh, M., & Kwon, Y. W. (2016, June). An assessment of internet of things protocols for resource-constrained applications. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 1, pp. 555-560). IEEE.

Naik, N. (2017, October). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In *2017 IEEE international systems engineering symposium (ISSE)* (pp. 1-7). IEEE.

OASIS. (2012, October). Advanced Message Queuing Protocol 2012. *Version 1.0 OASIS Standard.* Retrieved September 2, 2021, from http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-overview-v1.0-os.html.

Ramirez, J., & Pedraza, C. (2017, August). Performance analysis of communication protocols for internet of things platforms. In *2017 IEEE Colombian Conference on Communications and Computing (COLCOM)* (pp. 1-7). IEEE.

Saint-Andre, P. (2004). Extensible messaging and presence protocol (XMPP): Core.

Salman, T., & Jain, R. (2017). Networking Protocols and Standards for Internet of Things (Chapter 13). John Wiley & Sons, Inc.

Salman, T., & Jain, R. (2019). A survey of protocols and standards for internet of things. *arXiv preprint arXiv:1903.11549*.

Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015, April). Secure mqtt for internet of things (iot). In *2015 fifth international conference on communication systems and network technologies* (pp. 746-751). IEEE.

Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015, April). Secure mqtt for internet of things (iot). In *2015 fifth international conference on communication systems and network technologies* (pp. 746-751). IEEE.

Sonawala, N. M., Tank, B., & Patel, H. (2017, July). IoT protocol based environmental data monitoring. In *2017 International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 1041-1045). IEEE.

Soni, D., & Makwana, A. (2017, April). A survey on mqtt: a protocol of internet of things (iot). In *International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017)* (Vol. 20).

Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. *Wireless communications and mobile computing*, *2018*.

Tukade, T. M., & Banakar, R. (2018). Data transfer protocols in IoT—An overview. *International*

Journal of Pure and Applied Mathematics, *118*(16), 121-138.

Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing smart factory of industrie 4.0: an outlook. *International journal of distributed sensor networks*, *12*(1), 3159805.

Yassein, M. B., & Shatnawi, M. Q. (2016, September). Application layer protocols for the Internet of Things: A survey. In *2016 International Conference on Engineering & MIS (ICEMIS)* (pp. 1-4). IEEE.

Zamfir, S., Balan, T., Iliescu, I., & Sandu, F. (2016, October). A security analysis on standard IoT protocols. In *2016 international conference on applied and theoretical electricity (ICATE)* (pp. 1-6). IEEE.