Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 1399–1408

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

"A Novel MQTT Security framework In Generic IoT Model"

Chintan Patel[1,*], Nishant Doshi[1]

[a]*Pandit Deendayal Petroleum University, Raisan-367002, Gujarat, India*

Abstract

Internet of Things(IoT) emerges as a revolutionary technology since the last double decade. Internet of things has changed many aspects of the human. IoT has changed leaving styles and health care with the help of smart health care technologies like wearable devices. IoT has changed the power distribution mechanism in the smart grid environment where surplus renewable energy generated at the house or energy farm can also be distributed using a multi-dimensional grid and smart meters. One of the most beneficial aspects of IoT has emerged in the field of agriculture, wherewith the help of moisture and fertility sensor, the farmer can identify the need for fertilizer, quality of pesticides, quality of land, land moisture, and so on. Farmers can control the water distribution from home using smart sprinkling as well as pesticides sprinkling using IoT based drones. IoT makes use of light-weight communication with the motive of the reduction of extra overhead generated in regular internet communication. For to simplify and make faster communication IoT uses protocols like MQTT (Message queuing telemetry transport), COAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), REST (Representational State Transfer) and so on. The most famous protocol in the IoT communication at the application layer is the MQTT protocol, which makes use of TCP as an underlying transport layer protocol for the transmission. TCP based interface makes it more reliable protocol as well as a small header of MQTT protocol makes it suitable for IoT Eco-system, In this chapter, We have discussed the IoT, industry 4.0, impact of IoT on industry 4.0, MQTT Protocol, MQTT security aspects, Survey on various protocols used for to make MQTT Communication in a secured manner. We have surveyed many recent advances that happened for the MQTT Security and list out significant challenges in the IoT based industry faces when it comes to securing devices from physical as well as logical attacks. MQTT based device authentication, access control of resources, and security of communicated data over the insecure channel are some of the significant challenges that are discussed in depth. Overall this chapter will contribute in-depth security survey of IoT based industry 4.0.

Peer-review under responsibility of the scientific committee of the Third International Conference on Computing and Network Communications (CoCoNet'19).

Keywords: Internet of Things(IoT);MQTT;Authentication;Smart Home; Smart Grid

* Corresponding author. Tel.: +091-787-418-2588 ; fax: +0-000-000-0000.
* Chintan Patel
E-mail address: chintan.p592@gmail.com

Peer-review under responsibility of the scientific committee of the Third International Conference on Computing and Network Communications (CoCoNet'19).
10.1016/j.procs.2020.04.150

1. IoT and Industry 4.0

1.1. Internet of Things

In 1999, Kevin Ashton, a researcher working in MIT auto-id center, proposed the term ”The Internet of Things” for objects connected via RFID and other wireless technology. Internet of things was initiated with a broad aspect of connecting the world so that people can easily get ”any service” of ”any type” at ”any time” and ”anywhere.” The Internet of things market had shown multiplied exponential growth in the last decade. Quantity of connected objects had shown incredible growth in the recent past. Steve Symanovich from Symantec technology had provided a forecast about IoT devices. In 2016, he reported that currently, 4.7 billion devices are connected, which will grow to 11.6 billion devices and will reach 21 billion devices by 2025. [31]. As per other predictions are given by Intel, by 2020, there will be 200 billion total connected devices available in the world, which shows that an average of 26 smart objects will be there per person. Intel in the same report predicted that the internet of things based market might reach to 6.2 trillion USD by 2025 [13]. Another prediction by Kund Lasse Lueth in IoT-Analytics shows that by 2025, we will have more than 21.5 billion connected devices. IoT based market had already achieved 151 billion USD in 2018 and will reach to 1567 billion USD in 2025 [20]. Out of 29 billion devices that might be connected with other, 18 billion devices will be IoT devices by 2022. Out of that, more than 1.5 billion devices will be cellular devices that might communicate with 5G or 6G technology [9]. The Internet of things has changed the life of every age of people from all over the world. From the child’s toy to elderly citizen devices, it has expanded its scope, and the most important technology which is playing a role in this transformation is ”Sensing technology.” Some of the examples of wireless sensor network which affected human life are :

- Measuring climate on the farm using sensors like temperature sensors, humidity sensors will help in increasing crop yield per square km as well as saving of water, electricity, fertilizer, and unnecessary efforts by farmers.
- Monitoring traffic on the road using internet-connected CCTV, GPS, an accelerometer can steer traffic away from jams, accidents, and construction zones. Internet-connected mobile devices and vehicles can alert emergency services if any accident type incident occurs.
- Detection of human presence using the motion sensor, CCTV camera, thermal sensor in homes and offices can help to reduce wasted power in HVAC and lighting.
- Smart electrical/gas/water metering system can help in optimizing utility distribution systems and reduce inefficiencies and leakage in distribution.

Many authors have proposed various reference model for the internet of things. The reference model helps the research community, user community, and all other participants to understand the working of IoT, starting from data collection to intelligent decision making. Over here, we will go through the most widely accepted, adopted, and applied reference model proposed by CISCO, as shown in figure 1. [7][25][24].

- **Physical Devices and Controllers:** This is a bottom-most layer which is responsible for data collection. Sensors, microcontrollers, microprocessors, actuators will be deployed at this level. These devices will collect the data and forward it for further processing. This layer makes sure that the collected data is accurate and highly precise so that further processing will be easy.
- **Connectivity:** This layer takes care of communicating protocols. Communication between sensor devices and microcontrollers will be via RFID, BLE(Bluetooth Low Energy), NFC(Near field communication), Zigbee, and so on. It may also be possible that sensors are directly connected with microcontrollers via a cabled connection. Microcontroller and microprocessors will use protocols like MQTT(Message queuing telemetry transport), CoAP(Constrained application protocols) to communicate data to Gateway. Gateway will further use HTTP, MQTT, or CoAP to further store into the cloud or server.

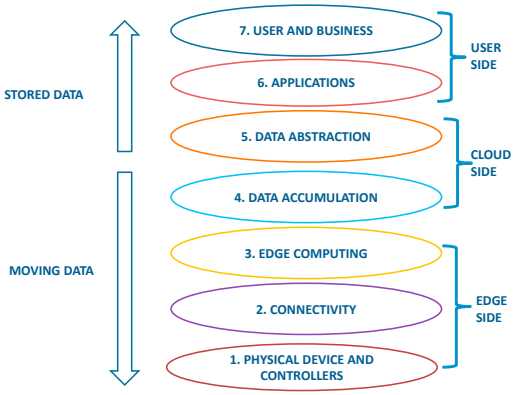

Fig. 1: CISCO 7 layered reference model[7]

- **Edge computing:** Edge computing is also called fog computing in the CISCO term. The primary objective of edge computing to perform raw data processing on the data. The gateway device will perform edge computing. Gateway device will low level data mining to discard unnecessary data and convert heterogeneous data into such a form, so that decision making becomes easier for machine learning algorithms and mining algorithms.
- **Data Accumulation,:** Data accumulation layer, will perform acquiring data from gateway device and store in to cloud for further processing.
- **Data abstraction:** Data abstraction layer will implement various data mining algorithms to get intelligent information.
- **Application:** At this layer, smart application dashboards are deployed either in the form of the mobile application or any other application. Smart health care, smart industry monitoring, smart row material management. This application will get data from the cloud. Based on requests, the cloud service provider will operate on data so that the user can get useful information. Some of the smart machines can deploy the built-in application and get the data from the cloud, and it can help them to perform machine learning algorithms.
- **User and Business:** This layer discusses the user's management and business management aspects of the wholly deployed application.

We have discussed the CISCO Reference model from bottom to up due to its real-time deployment flow in various applications. In most of the IoT application, implementation starts with the physical layer. Now we will discuss the industrial internet of things(IIoT), which is also called as industrial internet of things in broad aspects. Internet of things is combinations as well as permutations of many different devices, communication protocols, front-end applications, back-end applications, infrastructure, and so on. Authors in [4] and [21] had discussed the essential aspects of the internet of things in detail. Both the paper had discussed the need for IoT in industries, major communication protocols, types of devices that can play a role, significant challenges in IoT deployment, and futuristic aspects of IoT. Major sectors that can get the advantage of IoT for smooth manufacturing and easy distribution are :

- Healthcare Industry
- Education Industry
- Manufacturing Industry
- Transport Industry
- Pharmaceutical Industry
- Logistic Industry
- Agriculture Industry
- Mining Industry
- Security and surveillance

We will discuss the need for IoT in these industries one by one[32].

1. In major death occurred due to health issues, more challenging reason is **"delay in service"**. In the health-care, late diagnosis of the patient, delayed identification of disease, tracking live patient health, tracking chemical reactions occurred in the body due to medicine, quality of medicine, on-time supply of medication, and on-time availability of the human resource is a significant challenge that needs to tackle. In smart health-care, patient data is collected live via wearable sensors and supplied to the doctor database for live monitoring.
2. Education industry focusing on internet of things and its related technology to develop the youth, to track the education quality of the teacher, to monitor the health of student in campus, to guide the parents about the behaviour of their child on campus, to help parent to trace live location of their child and so on. Quality of cleanliness and environment inside campus can be monitored by using various bio-sensors, smell sensors, GPS devices, and CCTV cameras connected with the internet.
3. Production process in the industry involves many different stages starting from raw material collection too packed product. Every stage consists of the need for smart technology to improve the efficiency, accuracy, and quality of processing. The use of smart sensors to identify the need for raw material input can help to prepare base material for the product, and smart actuators can be used to force the tool to work based on predefined smart algorithms. Monitoring the quality of products using sensors, tracking product packaging using RFID can help to increase the speed of manufacturing.
4. Designing and manufacturing smart vehicles can improve services like logistics and public transportation. Companies like BMW has started production of a smart car with the capability of live GPS tracking, live engine quality monitoring, monitoring the live inner environment of the vehicle. Vehicles which are used for logistics purpose need smart technologies so that transportation authority can track the location of vehicle, can monitor the movement, suggest the vehicle driver a better route based on live traffic, follow the quality of product inside container, maintain the inside environment of container to preserve the quality of product and so on. The major challenge through which the logistic industry and transportation industry passes during the adoption of IoT is Security and Privacy.
5. Safety of mining workers is a significant concern in the mining industry. Sensors can be used to sense mine disaster signals to generate early warnings of futuristic disasters. Geographical sensors and geographical history data can be used for earlier production of disaster. Mining companies can use chemical and biological sensors that can be used for early disease detection and diagnosis health of workers working in the mining industry. The major technological challenge in the mining industry is in time communication between the upper surface and underground location.

The essential objectives of industry 4.0 are flexibility, decentralization, resource efficiency, digitization and networking, and miniaturization [16]. A cyber-physical system can be defined as "connecting physical manufacturing with the cyber world." The integration of the cyber-physical system in industrial production is a challenging task. Authors in [19] surveyed in detail about the adoption of a cyber-physical system in industry 4.0. Authors in [19] highlighted other industries like 3D Printing, Robotics, energy sector, aircraft transportation, battlefield live surveillance, maritime, chemical, and food supply chain where CPS has changed environment and economy of the industry. The major challenge in the cyber-physical system based industry is cyber attacks like denial of service attack. Due to the hierarchical work of the maximum industry in which the current stage is wholly dependent on the previous one, and the behavior of the next stage will also be dependent on the current stage output. So, cyber attacks at any stage (there is a chance that all stages may be connected with the internet). Another major challenge in the internet of things and the cyber-physical system is standardization of complete farm to plate production [1].

2. MQTT Protocol

2.1. Introduction

In the history of the internet, the most famous protocol is HTTP(Hypertext transfer protocol). The HTTP protocol has played a tremendous role in data transmission in this heterogeneous internet system. The difference which makes the internet of things separate from the internet is quantity and heterogeneity of IoT devices compare to internet devices. As we discussed in chapter 1, the number of IoT devices will be vast compared to the internet, and it may not be

easy to communicate efficiently using HTTP due to limitations like header size, latency, fully connection-oriented architecture, and so on. A comparison between MQTT, CoAP, HTTP, XMPP, and other protocols is discussed in detail in [22]. To limit the scope of the chapter, we will discuss the MQTT Protocol and its various applications.

MQTT protocol was derived by IBM [12], [5]. The basic difference between HTTP and MQTT is the communication model. HTTP communicates via the Request-Response model while the MQTT communicates via Publish-Subscribe model 2.

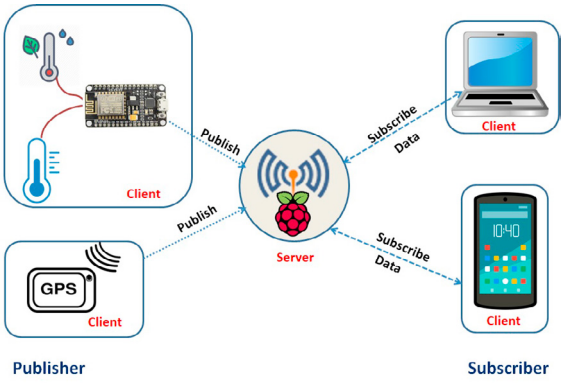

Fig. 2: MQTT Protocol working

As shown in figure 2, Very generalized internet of things deployment contains sensors, dashboard, or mobile applications. Acquired data passes through many switches and routers. In MQTT Protocol, three major entities are involved,

- first entity is **publisher**. Publisher collects the data from various sources like deployed sensors in machines or wearables, built-in mobile sensors, and so on. Publishers will publish data on a particular topic. Let us say the temperature sensor deployed in the home bedroom publishes data on the topic: ”/home/bedroom/temp-sensor.”
- Second entity is **Subscriber**. Subscriber specifically subscribes to the topic on which publisher is publishing a data. The subscriber can be a mobile application or user dashboard. Let us say the mobile application of user subscribes on the topic on deployment: ”/home/bedroom/temp-sensor.”
- Third and the most important entity are **broker**. Basic work of broker is to collect the data from the publisher and supply to subscriber. One of the famous brokers is [17]. The broker will be deployed on the intelligent and resourceful device so that it can handle multiples topics at a time. In most applications, Brokers store data in cloud services, and the user gets via it, so data processing can also become easy.

MQTT protocol makes use of 3 types of quality of service for communication. Quality of service in MQTT provides understanding between publisher and subscriber about the confirmation of data arrive.

- **QoS - 0:** Data will be communicated for at most once.
- **QoS - 1:** Data will be communicated for at least once.
- **QoS - 2:** Data will be transmitted precisely once.

2.2. Applications

MQTT Protocol is used in most of the iot application for data transmission. Some of the applications of MQTT protocol is as follows:

- **Smart Healthcare:** In smart health-care system, publisher senses the heart bit, blood pressure and other health-related parameter using sensors like EEG and ECG and send to the subscriber using MQTT [33],[2].

- **Smart Home:** In the smart home system, various sensors like temperature, light, motion, gas sensor, and cameras are deployed, which are connected with micro-programmers. Micro-programmers collect the data and communicate that data to the homeowner via the gateway using MQTT protocol [10], [14].
- **Smart Industry:** Machine to machine communication plays a significant role in the smart industry system. Optimization of material requirement, reduction of latency in decision making, identification of necessary objects are some of the vital needs of today's industry. MQTT can play a crucial role in the smart industry due to its small header size and simpler communication model [29],[15].
- **Smart Parking:** In a smart parking system, technology like RFID plays a significant role. RFID does not require to be placed in front of the scanner. RFID tags and RFID readers are two essential components. RFID reader reads tag and publishes that using MQTT to store in to cloud. The user of the smart parking system can easily detect whether the location is empty or not [8].
- **Smart weather monitoring:** Smart weather system works on various sensors like wind speed sensor, solar radiation sensor, air pressure sensor, temperature sensor, humidity sensor. MQTT protocol can also be used in a smart weather system for communication [28].

3. MQTT Authentication Framework

3.1. Related Work

In [3], authors have discussed various attack vectors and security analysis of complete MQTT protocol. Authors have highlighted various loopholes in MQTT communication where the attacker can try to attack. Authors in [30] discussed attribute-based authentication, authors in [6] had proposed authentication mechanism based on the token generation and token distribution, Authors in [27] have discussed identity-based authentication mechanism, authors in [18] have made use of elliptic curve cryptography to design authentication algorithms and security key generation. In [11], authors have proposed an updated light-weight version of the famous o-Auth protocol for authentication. MQTT Security is important part of IoT secure communication[26]. Motivation behind this proposal is to put forward a novel idea for designing new security framework and make use of it.

3.2. Proposed Framework

In this subsection, we propose a new framework for MQTT based user authentication[23]. The proposed framework consists of three phases. The phases include the user registration phase, the device registration phase, and the user authentication phase. As per the discussed above, MQTT communication involves three entities. The entities include publisher, subscriber, and a broker. In the proposed model, we consider that the user wants to access the data from the sensing device. For that, both user device and sensing device do the registration with the broker device and later on user device authenticate with the broker device for to get the sensor data.

3.2.1. User Registration Phase

In this phase, as shown in Figure. 3, the user communicates with the broker for registration with the user credentials. This phase works as follows:

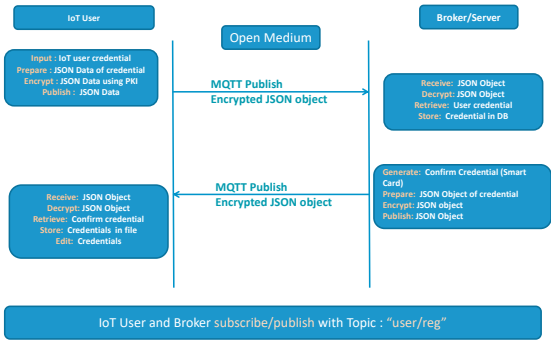

Fig. 3: MQTT Authentication Framework : User Registration

- The user generates a message with the user credentials and encrypts this message with the pre-shared public key of the broker device. The user publishes this message to broker over the open channel
- The broker retrieves the user credentials by decorating it using the private key. The broker store the credential in the database. The broker generates other necessary credentials needed by the user to prove authenticity. The broker creates a credential object, encrypt these object and publish it on the public channel.
- The user retrieves the credentials computed by the broker, validate the broker, and store the credentials in the file. The user can also store in the database if the user is a resource capable computing device.

3.2.2. Device Registration Phase

In this phase, as per shown in Figure. 4 the device communicate with the broker for registration with the device credentials. This phase works as follows:

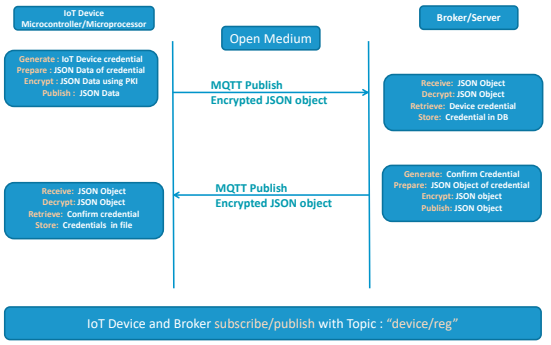

Fig. 4: Device Registration

- The sensing device generates a message with the sensing device credentials and encrypt this message with the pre-shared public key of the broker device. The sensing device publishes this message to broker over the open channel
- The broker retrieves the sensing device credentials by decorating it using the private key. The broker store the credential in the database. The broker generates other necessary credentials needed by sensing device to prove the authenticity. The broker creates a credential object, encrypt these object and publish it on the public channel.
- The sensing device retrieves the credentials computed by the broker, validate the broker, and store the credentials in the file. The sensing device can also store in the database if the sensing device is a resource capable computing device.

3.2.3. User Authentication Phase

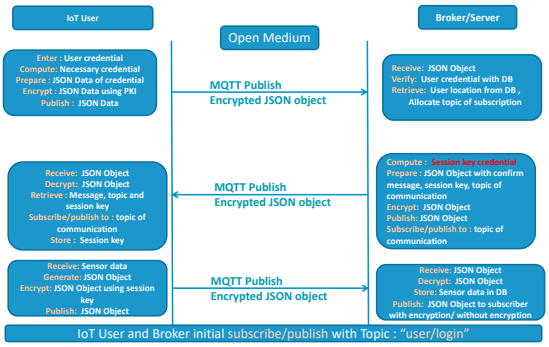

Fig. 5: User Authentication

In this phase, as per shown in Figure. 5, the user authenticate himself/herself with the broker. This phase is performed as follows:

- The user provides user credentials, and the user device computes the necessary credentials. The user device encrypts the computed credentials and creates a JSON object. The user device publishes this JSON object to the broker.
- The broker device retrieves the user credentials and validate the identity of the user in the database. The broker allocates the valid topics to the user to receive the data from the sensing devices. The broker also computes the session key credentials that may be needed by the user for secure communication with the sensing device. The broker creates a JSON object with the confirm message, session key, and topic of communication and encrypts it with the public key of the user device. The broker publishes this JSON object to the user device. The broker also shares user identity and session keys with the sensing devices in a secured manner.
- The user retrieves the valid topic to subscribe to each sensor and the session key. The user subscribes to the allocated topics and stores the session key. It starts receiving the data from the sensor in the session key encrypted manner. The user encrypts those data and stores it into either a local database or into a broker database through the public channel.

The above proposed framework is generalized framework and can be used by other cryptographic protocol designer for designing full proof secured MQTT communication.

4. Conclusion

In this paper, we have discussed basics about the internet of things, application of the internet of things in various industries. MQTT(Message queuing telemetry transport) is the most crucial protocol which is used for IoT application layer communication. Security and privacy are a significant challenge that all the major industries are facing nowadays, so in this paper, we have highlighted various aspects of security like access control and authentication. At last, we have highlighted various related research work and proposed a novel authentication framework for MQTT based communication.

References

[1] 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, 4674–4682. doi:10.1109/TII.2018.2855198.

[2] and, and, 2016. Design and implementation of mobile health monitoring system based on mqtt protocol, in: 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp. 1679–1682. doi:10.1109/IMCEC.2016.7867503.

[3] Andy, S., Rahardjo, B., Hanindhito, B., 2017. 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. doi:10.1109/EECSI.2017.8239179.

[4] Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: A survey. Computer Networks 54, 2787 – 2805. URL: http://www.sciencedirect.com/science/article/pii/S1389128610001568, doi:https://doi.org/10.1016/j.comnet.2010.05.010.

[5] Banks, A., Gupta, R., 2014. Mqtt version 3.1. 1. OASIS standard 29, 89.

[6] Bhawiyuga, A., Data, M., Warda, A., 2017. Architectural design of token based authentication of mqtt protocol in constrained iot device, in: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–4. doi:10.1109/TSSA.2017.8272933.

[7] CISCO, 2014. The internet of things reference model URL: http://cdn.iotwf.com/resources/71/IoT-Reference-Model-White-Paper-June-4-2014.pdf, arXiv:http://cdn.iotwf.com/resources/71/IoT-Reference-Model-White-Pa

[8] Dhar, P., Gupta, P., 2016. Intelligent parking cloud services based on iot using mqtt protocol, in: 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 30–34. doi:10.1109/ICACDOT.2016.7877546.

[9] ericsson, 2018. The connected future. URL: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.

[10] Froiz-Míguez, I., Fernández-Caramés, T., Fraga-Lamas, P., Castedo, L., 2018. Design, implementation and practical evaluation of an iot home automation system for fog computing applications based on mqtt and zigbee-wifi sensor nodes. Sensors 18, 2660.

[11] Hardt, D., 2013. The oauth 2.0 authorization framework.

[12] Hunkeler, U., Truong, H.L., Stanford-Clark, A., 2008. Mqtt-s a publish/subscribe protocol for wireless sensor networks, in: 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), pp. 791–798. doi:10.1109/COMSWA.2008.4554519.

[13] INTEL, 2019. A guide to internet of things infographic. URL: https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

[14] Jamborsalamati, P., Fernandez, E., Moghimi, M., Hossain, M.J., Heidari, A., Lu, J., 2018. Mqtt-based resource allocation of smart buildings for grid demand reduction considering unreliable communication links. IEEE Systems Journal , 1–12doi:10.1109/JSYST.2018.2875537.

[15] Katsikeas, S., Fysarakis, K., Miaoudakis, A., Van Bemten, A., Askoxylakis, I., Papaefstathiou, I., Plemenos, A., 2017. Lightweight amp; secure industrial iot communications via the mq telemetry transport protocol, in: 2017 IEEE Symposium on Computers and Communications (ISCC), pp. 1193–1200. doi:10.1109/ISCC.2017.8024687.

[16] Lasi, H., Fettke, P., Kemper, H.G., Feld, T., Hoffmann, M., 2014. Industry 4.0. Business & Information Systems Engineering 6, 239–242. URL: https://doi.org/10.1007/s12599-014-0334-4, doi:10.1007/s12599-014-0334-4.

[17] Light, R.A., 2017. Mosquitto: server and client implementation of the mqtt protocol. The Journal of Open Source Software 2, 265.

[18] Lohachab, A., Karambir, 2019. Ecc based inter-device authentication and authorization scheme using mqtt for iot networks. Journal of Information Security and Applications 46, 1 – 12. URL: http://www.sciencedirect.com/science/article/pii/S2214212618306513, doi:https://doi.org/10.1016/j.jisa.2019.02.005.

[19] Lu, Y., 2017. Cyber physical system (cps)-based industry 4.0: A survey. Journal of Industrial Integration and Management 02, 1750014. doi:10.1142/S2424862217500142.

[20] Lueth, K.L., 2018. State of the iot 2018: Number of iot devices now at 7b market accelerating. URL: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b.

[21] Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. Ad Hoc Networks 10, 1497 – 1516. URL: http://www.sciencedirect.com/science/article/pii/S1570870512000674, doi:https://doi.org/10.1016/j.adhoc.2012.02.016.

[22] Naik, N., 2017. Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http, in: 2017 IEEE International Systems Engineering Symposium (ISSE), pp. 1–7. doi:10.1109/SysEng.2017.8088251.

[23] Patel, C., Doshi, N., . Cryptanalysis and improvement of barman et al.s secure remote user authentication. INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING 13, 604610. URL: http://naun.org/cms.action?id=19907.

[24] Patel, C., Doshi, N., 2018. Internet of things security: Challenges, advances, and analytics .

[25] Patel, C., Doshi, N., 2019a. Security Challenges in IoT Cyber World. Springer International Publishing, Cham. pp. 171–191. URL: https://doi.org/10.1007/978-3-030-01560-2-8, doi:10.1007/978-3-030-01560-2-8.

[26] Patel, C., Doshi, N., 2019b. Security challenges in iot cyber world, in: Security in Smart Cities: Models, Applications, and Challenges. Springer, pp. 171–191.

[27] Peng, W., Liu, S., Peng, K., Wang, J., Liang, J., 2016. A secure publish/subscribe protocol for internet of things using identity-based cryptography, in: 2016 5th International Conference on Computer Science and Network Technology (ICCSNT), pp. 628–634. doi:10.1109/ICCSNT.2016.8070234.

[28] Pooja, S., Uday, D.V., Nagesh, U.B., Talekar, S.G., 2017. Application of mqtt protocol for real time weather monitoring and precision farming, in: 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), pp. 1–6. doi:10.1109/ICEECCOT.2017.8284616.

[29] Shrouf, F., Ordieres, J., Miragliotta, G., 2014. Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm, in: 2014 IEEE International Conference on Industrial Engineering and Engineering Management, pp. 697–701. doi:10.1109/IEEM.2014.7058728.

[30] Singh, M., Rajan, M.A., Shivraj, V.L., Balamuralidhar, P., 2015. Secure mqtt for internet of things (iot), in: 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 746–751. doi:10.1109/CSNT.2015.16.

[31] Symanovich, S., 2016. The future of iot: 10 predictions about the internet of things. URL: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html.

[32] Xu, L.D., He, W., Li, S., 2014. Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics 10, 2233–2243. doi:10.1109/TII.2014.2300753.

[33] Yang, Z., Zhou, Q., Lei, L., Zheng, K., Xiang, W., 2016. An iot-cloud based wearable ecg monitoring system for smart healthcare. Journal of Medical Systems 40, 286. URL: https://doi.org/10.1007/s10916-016-0644-9, doi:10.1007/s10916-016-0644-9.