Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 194 (2021) 132–139

Procedia Computer Science

www.elsevier.com/locate/procedia

18th International Learning & Technology Conference 2021

Authentication mechanisms for IoT system based on distributed MQTT brokers: review and challenges

Hassan Kurdi[a]*, Vijey Thayananthan[b]

[a] *College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia*
[b]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*

Abstract

With the rapid growth of internet connected devices and the tremendous amount of data that could be generated and exchanged in IoT environment, we need to reconsider in the current IoT architecture that based on Cloud computing system, to avoid the issues related to performance and scalability. Message Queue Telemetry Transport (MQTT) is one of promising protocol for data exchange in IoT that could encounter such issues because it relies on central broker located in Cloud, and this may lead to increase network congestion, performance overhead or bottleneck. Therefore, we need to leverage Fog computing by developing a distributed architecture for MQTT that contain multiple brokers. In this case, IoT services can be coordinated and managed between Fog computing and Cloud computing. However, this will open new security challenges for several reasons. Firstly, security procedures need to be modified because MQTT that based on distributed architecture require additional multiple brokers and different communication standards that may increase security threats and increase security management complexity. Secondly, MQTT is inherently lacking efficient security features because it performs username/password-based authentication in a plain text, that protected by cryptographic protocol SSL/TSL which is not consider as lightweight protocol for resources constrained devices. This paper will present taxonomy and realization process of IoT authentication scheme. In addition, the paper will discuss challenges of applying authentication mechanisms for IoT systems that based on distributed MQTT brokers.

Keywords: MQTT; Authentication; Internet of things (IoT); Security; Distributed architecture; Fog computing

* Corresponding author. Tel.: +966148618888
E-mail address: hkurdi@taibahu.edu.sa

10.1016/j.procs.2021.10.066

1. Introduction

Handling and managing the large volume of data that are generated and transmitted in IoT environment, is critical issues affecting performance and scalability for Cloud-based IoT system. One of IoT protocol that could encounter such issues is Message Queue Telemetry Transport (MQTT) because it relies on a central broker locatedin Cloud for clients (publishers and subscribers) communication, and this may lead to increase network congestion, performance overhead or bottleneck issues. As a result, we need to leverage Fog computing by developing a distributed architecture for MQTT that contain multiple brokers. In this case, IoT services can be coordinated and managed between Fog computing and Cloud computing. Fog computing was adopted recently as a complementary technology with Cloud computing to provide some specific characteristics, such as low-latency, location awareness, geo-distribution, increased data security and real-time processing, [1]. In addition, it aims to bring computing, storage and network capabilities closer to the end-users.

However, building a distributed architecture for MQTT with multiple brokers will open new security challenges for many reasons. Firstly, security procedures in distributed architecture is not similar to the procedures in centralized architecture, because the way of delivering data from publisher to subscriber will be modified, especiallyif they are connected to two different brokers. Additionally, communication between brokers itself, which is not exist in traditional MQTT, need to implement security properties such as authentication. Secondly, MQTT is inherently lacking efficient security features because it performs username/password-based authentication in a plain text, and this in turn can result in different kind of attacks such as impersonation, eavesdropping and replay attack. Moreover, this username/password protected by SSL/TSL which is not consider as lightweight protocol for resources constrained devices.

To best of our knowledge, authentication mechanisms of MQTT that based on multiple brokers has not been investigated as required by researchers, and we need to develop a new authentication mechanism that compatible with the distributed architecture of MQTT to ensure security of clients and brokers. However, there are many questions arise and need to be solved such as: how data through two or more different brokers can be delivered between MQTT clients (from publisher to subscriber), how can we manage authentication between clients and brokers communication and between brokers communication and how can we maintain system performance and provide scalability while implementing authentication requirements. This paper will review the current studies related to authentication and distributed architecture of MQTT and show their limitations. The paper aim to discuss challenges for MQTT authentication that based on distributed multiple brokers. The contribution of this paper is as following:

- We provide a taxonomy and realization process of authentication scheme in Internet of Things (IoT).
- We present the common cyber-attacks for IoT authentication explaining how these attacks threat MQTT that based on multiple brokers.
- We discuss the challenges related to authentication scheme including its performance and scalability for MQTT that based on multiple brokers.

The paper is organized as following: background in section 2, provide introduction of MQTT protocol moreover, present taxonomy and realization processes of IoT authentication. Section 3 present related work of current authentication mechanisms and distributed architectures of MQTT. Section 4, highlight the most common attacks that can threat significantly IoT authentication systems. Section 5, discuss the challenges of developing authentication scheme for MQTT based on multiple brokers.

2. Background

2.1. Message queuing telemetry transport protocol (MQTT)

MQTT is a messaging protocol based on publish/subscribe model that allows multiple clients (publishers and subscribers) to communicate with each other through central broker. It is one of the IoT application layer protocols that feature with lightness, flexibility and simplicity, because the required number of messages exchanged for each connection is few and the essential header of packets is small as well as there are optional provided services such as controlling quality of service level (QoS) and implementing secure connection. These features make MQTT suitable for resource-constrained devices, low bandwidth and high latency networks. The protocol is ideal for mobile IoT applications and machine-to-machine (M2M) communication. MQTT uses TCP protocol at the transport layer, and rely on five main components: publisher, subscriber, broker, message and topic:

- Publisher: the device who send data of a specific topic to the broker.
- Subscriber: the device who request and receive the data of topic(s) that interested in, from the broker.
- Broker: the server who receive the data of topics that sent by publishers, and send it to the subscribers who interested in that topics.
- Messages: there are 14 type of messages that sent to and received from broker. The key messages include CONNECT and CONNACK which connect the clients with the broker, as well as SUBSCRIBE/SUBACK which allow client to subscribe to topic, while PUBLISH/PUBACK allow sending data of the topic from publisher to broker or from broker to subscriber.
- Topic: it is a form of addressing and structured in a hierarchy similar to folders in a file system using the forward slash (/) as a separator. The topic can contain wildcard characters to allow client to subscribe multiple topics at once.

2.2. Taxonomy of IoT authentication

This section presents a taxonomy of IoT authentication scheme using a collection of criteria selected based on similarities and fundamental characteristics of the implemented current schemes in IoT. There are 6 criteria will be summarized as following:

2.2.1. IoT layers

Each layer (perception, network and application) in IoT architecture prone to different kind of attacks. Thus, authentication considered a core security requirement for all IoT layers, [11].

- Perception layer: contain sensors which need node authentication to prevent such as replay attack and forgery attack.
- Network layer: in which data transmission and routing occur, vulnerable to eavesdropping and MITM attack.
- Application layer: which based on messaging protocols such as MQTT and CoAP, is responsible for delivering IoT services to users which require to be authenticated.

2.2.2. Architecture

- Centralized: using a single server or a trusted third party to distribute, manage and validate the credentials used for authentication.
- Distributed: using multiple distributed servers to authenticate devices in parallel, and this lead to reduce computation and communication overhead of authentication process, [12].

2.2.3. Cryptographic methods

- Cryptographic hash functions: It is the method where plaintext is converted to ciphertext, and when hash function is applied to a message of any bit length, the result will be a digest (hash value) of a fixed length.
- Symmetric key authentication: The encryption process in this method rely on using the same key for encryption and decryption.
- Asymmetric key authentication: It is also called public-key cryptography, in which the encryption and decryption process use two different keys namely, public key which could be shared among system's users, and private key which is known only by the owner.

2.2.4. Authentication procedures

- One-way authentication: where one entity authenticates the credentials of other entity.
- Two-way authentication: it is called mutual authentication, in which both entities authenticate each other.

- Three-way authentication: where the authentication server verifies the two communicated entities, in addition allow them to mutually authenticate each other.

2.2.5. Authentication factor

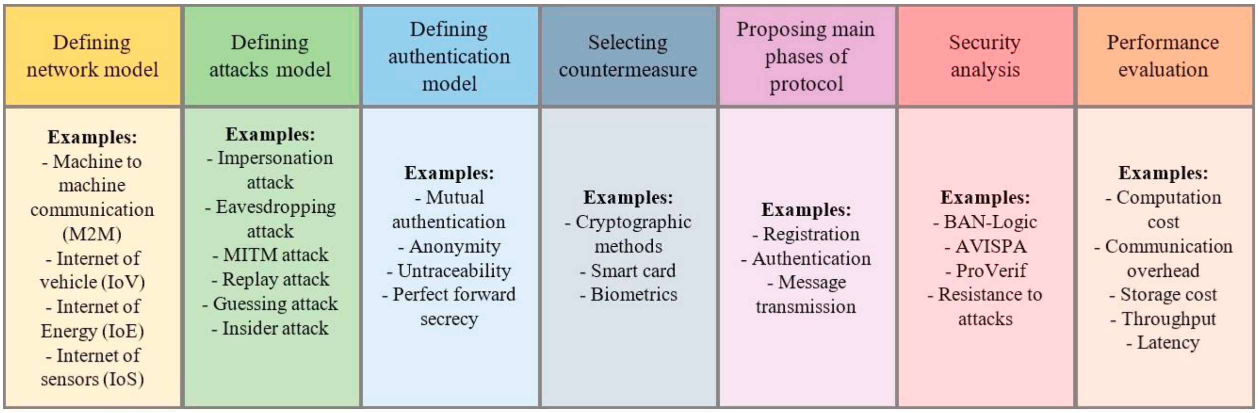
- One factor: it is the authentication process that based on one piece of evidence to represent the user or IoT device, such as username/password or ID, respectively.
- Two factors: where two pieces of evidence should be presented to authenticate the entity. For example, using ID and smart card or using username/password with biometric.
- Three factors: it is mean the entity should provide three pieces of evidence to complete the authentication process. For instance, using ID, smart card and biometric together.

2.2.6. Authentication token

- Soft token: it is software-based token that generate a piece of data used one time to prove user/device identity. Examples, challenge response token such as (nonce, random number and pseudo-number) and One-time password (OTP).
- Hard token: it is hardware-based token contain a chip that store authentication parameters, such as cryptographic keys to generate digital signature. Examples, smart card, dongle and radio-frequency identification (RFID).

2.3. Realization process of IoT authentication

This section describes the processes that should be considered to ensure that authentication scheme has the appropriate design and behavior to meet functional requirements for the system. According to [13] the realization processes of IoT authentication scheme are shown in Fig. 1.



Defining network model	Defining attacks model	Defining authentication model	Selecting countermeasure	Proposing main phases of protocol	Security analysis	Performance evaluation
Examples: - Machine to machine communication (M2M) - Internet of vehicle (IoV) - Internet of Energy (IoE) - Internet of sensors (IoS)	**Examples:** - Impersonation attack - Eavesdropping attack - MITM attack - Replay attack - Guessing attack - Insider attack	**Examples:** - Mutual authentication - Anonymity - Untraceability - Perfect forward secrecy	**Examples:** - Cryptographic methods - Smart card - Biometrics	**Examples:** - Registration - Authentication - Message transmission	**Examples:** - BAN-Logic - AVISPA - ProVerif - Resistance to attacks	**Examples:** - Computation cost - Communication overhead - Storage cost - Throughput - Latency

Fig. 1. Realization process of IoT authentication

3. Related work

This section briefly reviews the current studies related to MQTT protocol, classifying them into three parts based on those involving only authentication property, those involving only multiple brokers and finally those encompassing authentication property and multiple brokers.

The studies that only focused on authentication mechanisms for MQTT, the study in [2] introduced a lightweight authentication mechanism by implementing token-based authentication and using the secret key for encryption and decryption. The secret key is periodically updated using chaotic algorithm to provide high diversity among consecutive security keys. However, updating the key frequently by broker could cause communication and processing overhead. The paper in, [3] presented a lightweight security solution using Elliptic Curve Cryptography

(ECC) for publish-subscribe protocol based on Fog computing. The solution provided mutual authentication and encryption system. One of the system disadvantages is that keys management and keys revocation issues were not addressed [4], thus implementing this solution could be a complicated operation in distributed architecture. In addition, Fog broker is not scalable and prone to performance overhead or bottleneck. The study in [5] proposed a lightweight authentication and authorization framework for inter-device communication in distributed environment using ECC with Transport Layer Security (TLS). The system utilized the concept of MQTT protocol using single broker to broadcast data. There is high computation cost for authentication server in term of hashing, encryption and decryption, and this cause performance overhead. In addition, the increase number of devices communication could cause broker bottleneck. The author in [6] provide security scheme to achieve devices and data authentication including data encryption, for end to end IoT devices communication in publish-subscribe model. The proposed architecture adopts fog node which compose of the broker and registration authority (RA). Although the scheme was outperformed TLS in term of storage and communication overhead, the broker could prone to single point of failure.

Regarding studies that proposed distributed architecture for MQTT without focusing on security solutions. In [7], the author proposes MQTT with a multicast mechanism DM-MQTT (Direct Multicast-MQTT) to minimize data transfer delay and network congestion for the massive IoT communications in distributed edge networks. This architecture does not apply any security solutions such as authentication and authorization. The study in [8] present Interworking Layer of Distributed MQTT brokers (ILDM), which enables multiple MQTT brokers to cooperate with each other. The system is prone to different kind of attacks such as impersonation, MITM and replay attack, due to there is no security solutions are presented. The author in [9] propose Edge-Cloud pub/sub broker model that allow multiple broker to dynamically coordinate among each other for data delivery to achieve high scalability and low latency properties in large-scale IoT system. The model depends on coordination servers to manage subscription and publication requests among the brokers. The proposed model did not involve any security solutions.

Regarding studies that proposed security solutions for MQTT based on multiple brokers, the paper in [10] proposed a secure and scalable MQTT communication framework for industrial IoT based on multi-stage brokers which contain three level of brokers. The paper focused more on authorization by enabling clients to access topics from different brokers and interoperability by deploying dynamic bridging mechanism to enable brokers communicate each other. The limitations of this framework are, there is a centralized AS which can cause single point of failure and bottleneck. The cryptographic method is based on 2048-bit RSA which is not consider a lightweight algorithm for resource constrained devices, and cause high computation and communication overhead. Lastly, the paper did not focus on improving authentication mechanism.

4. Cyber-attacks for MQTT based on distributed multiple brokers

Implementing MQTT in a distributed environment with multiple brokers, increase authentication breaches and authentication management complexity, due to new modification requirements such as communication methods, system architecture. In other words, suppose we have multiple brokers distributed in Fog layer and broker in Cloud layer as shown in Fig. 2, thus the communication will not only be restricted between IoT devices and the broker in Cloud as traditional MQTT, the communication will be established between brokers itself. Therefore, each communication, component and layer vulnerable to cyber-attacks. According to [14], there are 35 attacks can threaten the security of IoT. The most common attacks that are evaluated to verify the functionality of authenticationprotocols are, man in the middle (MITM) attack, impersonation attack and replay attack, which will be focused in this paper.

4.1. Man-In-The-Middle attack

It is an attack where adversary intercepts the communication between two legitimate entities to eavesdrop or modify the exchanged messages. Unlike, traditional MQTT where attack only target the communication between client and the single broker in Cloud, In distributed MQTT architecture, there are several parts of the system can be exploited by adversary such as the communication between clients and brokers, between brokers in Fog and Cloud and between brokers in the same layer.

4.2. Impersonation attack

In this attack, the adversary tries to masquerade as a legitimate user/device by obtaining authentication request message using power analysis or succeeding to perform MITM or replay attack. In distributed MQTT architecture, any node (IoT device and broker) in any layer (device, Fog and Cloud) can be impersonated, and this may result in serious issues such as controlling message exchanging, manipulating the value of publishing data, subscribing to unauthorized topics.

4.3. Replay attack

It is the attack where the adversary captures the login information of a legitimate entity, then this information can be resent to the entity who responsible for authentication. For example, in mutual authentication, adversary can deceive either the client or broker by reusing and sending the credentials of one of them. In this case, the adversary will obtain all privilege dedicated to the legitimate entity.

5. Challenges and discussion

Focusing on the architecture in Fig. 2, data transmission between publishers and subscribers could be performed through one broker, or multiple brokers, and this is determined based on the broker(s) that the clients connected to. For example, if the publisher and subscriber connected to the broker (B1), the process of delivering data will be conducted by the broker (B1). While, if the publisher and subscriber connected to two different brokers (B1) and (B2), respectively, in this case, data need to be transmitted through more than one broker. The issue is, each client requesting and sending data and each broker participating in delivering data to destination must be authenticated, and at the same time we need to maintain performance, reduce latency and achieve scalability. As a result, there are several challenges will be discussed, as following:

5.1. Broker communication approach

It is axiomatic that clients in Fog-based distributed architecture for MQTT connect to different brokers. However, delivering the data from publisher to subscriber that connect two different brokers is a challenge, because data may need to pass through more than one broker, and this may lead to high probability of transmission delay. In addition, the client's communication to brokers must be managed in a way that prevent the increased connection load which may lead to traffic congestion and bottleneck issue on a specific broker. Furthermore, the long route the data take to reach its destination the higher risk is caused. For example, the security threats of transmitting data through three brokers higher than transmitting them through one broker, because the number of establishing communication among brokers will be higher, which increase the chance of exploiting these communications by the attacker. As a result, we need to reduce the number of times data travels between brokers and at the same time we need to maintainload balancing of receiving connection requests to brokers.

5.2. Scalable authentication

Authenticating numerous numbers of publisher and subscriber connected to multiple brokers require an authentication scheme that achieve scalability. Developing authentication scheme for distributed architecture of MQTT is a complicated issue because each node (publisher, subscriber and brokers) participating in publishing data and subscribing to topics should be mutually authenticated, and this increase the complexity of managing authentication process, as well as, this can increase the overhead of the authentication server which result in bottleneck by sending many authentication requests at the same time. In addition, the server prone to single point of failure and network congestion which cause data loss. Therefore, we need scalable authentication architecture to prevent such issues.

5.3. Lightweight cryptographic method

Due to the limited computing power, memory size, storage space and energy capacity, the use of traditional cryptographic methods will not be suitable for authentication process of resource constrained IoT devices. With non-lightweight cryptographic mechanisms, all these resources of devices will be highly consumed during authentication process. Therefore, we need a lightweight cryptographic algorithm that use smaller key size, less bandwidth and faster encryption, decryption and key generation operation, to reduce computational and communication overheads.

5.4. Data integrity

Data integrity is a fundamental property in authentication process, because it confirms correctness of credentials of nodes, and they have not been manipulated by any adversary. Ensuring data integrity in Fog-based distributed architecture for MQTT is an issue worthy of attention, because each time the connection is establishes between any nodes participating for delivering data to destination, need to verify the credential mutually to ensure that it has not been altered. For example, suppose that publisher "P1" connect directly to broker "B1" and subscriber "S1" connect directly to broker "B2", thus data will transmit from "P1" to "B1" then to "B2" and finally to the destination "S1". During this data transmission, the credential of data sender and receiver need to be mutually verified. One of the most common method of cryptography used to provide integrity is hash function (such as SHA-1 and SHA-2).

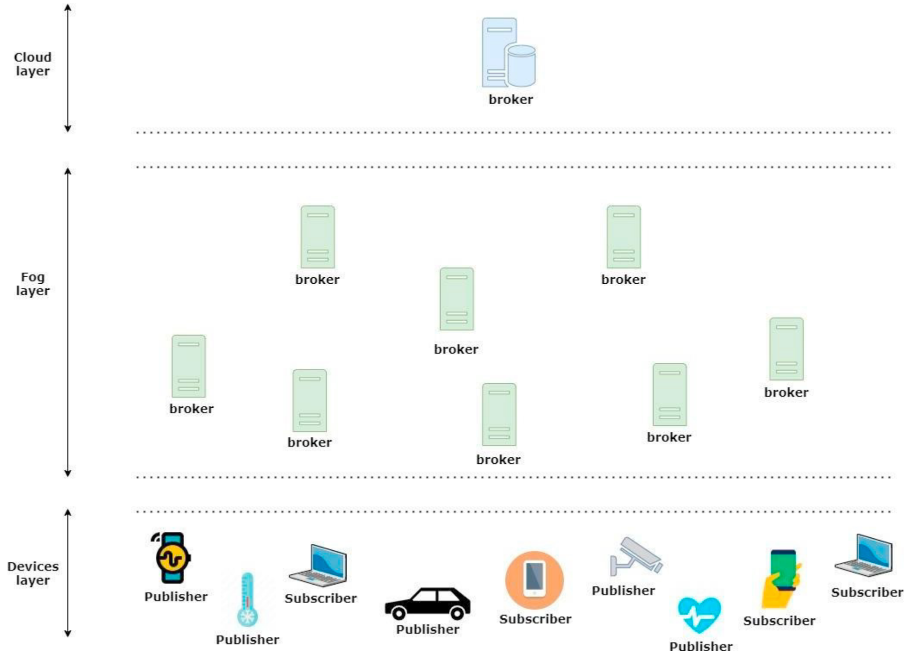


Fig. 2. Fog-based distributed architecture for MQTT

5.5. Cyber-attack resistance

Undoubtedly, that the goal of applying authentication scheme is protecting system from attacks that breach identity or credentials of entities. This paper focused on most common attacks namely, impersonation, replay and MITM attack that can be relied on to evaluate authentication mechanisms. Although developing a distributed architecture for MQTT improve performance and scalability, the opportunities of attacks and the complexity of managing these attacks will be increased, because vulnerabilities that can be exploited increase. For example, in Fog-based distributed architecture for MQTT, the communication between IoT devices and brokers, betweenbrokers in Fog and Cloud and between brokers in Fog, all prone to replay and MITM attacks, thus any entity can be impersonated and pretend to be a legitimate clients and brokers.

6. Conclusion

The expectations of the rapid grow of internet connected devices and the extensive applications of IoT has drawn attention of researchers to consider in scalability and performance related issues for IoT systems. Undoubtedly, many researches heading to proposing and building distributed architecture solution for IoT systems to solve such issues. However, this will open new security challenges ranging from attacks on entities to attacks on data that exchanged. One of IoT messaging protocol that encounter these challenges is MQTT.

Therefore, this paper discusses challenges of developing a distributed architecture and applying an authentication schemes for MQTT protocol that based on multiple brokers. To best of our knowledge, authentication requirements of such architecture of MQTT has not been investigated as required. This paper would help researchers to identify authentication related challenges such as scalable authentication, cryptographic methods, data integrity and attack resistance. In addition, by presenting taxonomy and realization process, there would be a clear perception about requirements and followed procedures for IoT authentication scheme.

For future work, we are going to develop MQTT protocol that based on distributed MQTT brokers for IoT system and address the challenges that have been discussed previously in this paper. During the research we will present the evaluation and results.

References

[1] Kahvazadeh, Sarang, Vitor B. Souza, Xavi Masip-Bruin, Eva Marn-Tordera, Jordi Garcia, and Rodrigo Diaz. (2017) "Securing combined fog-to-cloud system through SDN approach." In Proceedings of the 4th Workshop on CrossCloud Infrastructures & Platforms: 1-6.

[2] Bali, Ranbir Singh, Fehmi Jaafar, and Pavol Zavarasky. (2019) "Lightweight authentication for MQTT to improve the security of IoT communication." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy: 6-12.

[3] Diro, Abebe Abeshu, Naveen Chilamkurti, and Neeraj Kumar. (2017) "Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing." Mobile Networks and Applications 22, no. 5: 848-858.

[4] Anantharaman, Prashant, Kartik Palani, and Sean Smith. (2019) "Scalable Identity and Key Management for Publish-Subscribe Protocols in the Internet-of-Things." In Proceedings of the 9th International Conference on the Internet of Things: 1-7.

[5] Lohachab, Ankur. (2019) "ECC based inter-device authentication and authorization scheme using MQTT for IoT networks." Journal of Information Security and Applications 46: 1-12.

[6] Diro, Abebe, Haftu Reda, Naveen Chilamkurti, Abdun Mahmood, Noor Zaman, and Yunyoung Nam. (2020) "Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication." IEEE Access 8: 60539-60551.

[7] Park, Jun-Hong, Hyeong-Su Kim, and Won-Tae Kim. (2018) "DM-MQTT: An efficient MQTT based on SDN multicast for massive IoT communications." Sensors 18, no. 9: 3071.

[8] Banno, Ryohei, Jingyu Sun, Masahiro Fujita, Susumu Takeuchi, and Kazuyuki Shudo. (2017) "Dissemination of edge-heavy data on heterogeneous MQTT brokers." In 2017 IEEE 6th International Conference on Cloud Networking (CloudNet): 1-7.

[9] Pham, Van-Nam, and Eui-Nam Huh. (2019) "An Efficient Edge-Cloud Publish/Subscribe Model for Large-Scale IoT Applications." In International Conference on Ubiquitous Information Management and Communication: 130-140. Springer, Cham.

[10] Amoretti, Michele, Riccardo Pecori, Yanina Protskaya, Luca Veltri, and Francesco Zanichelli. (2020) "A Scalable and Secure Publish/Subscribe-based Framework for Industrial IoT." IEEE Transactions on Industrial Informatics.

[11] El-hajj, Mohammed, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni. (2019) "A survey of internet of things (IoT) Authentication schemes." Sensors 19, no. 5: 1141.

[12] Li, Wei, Yong Dai, Weiwei Miao, Mingxuan Zhang, Jin Fan, Rui Liu, and Yang Li. (2020) "A Group-based End-to-end Identity Authentication Method for Massive Power Wireless Private Network." In 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC): 14-17.

[13] Srivastava, Astha, Shashank Gupta, Megha Quamara, Pooja Chaudhary, and Vidyadhar Jinnappa Aski. (2020) "Future IoT ‐ enabled threats and vulnerabilities: State of the art, challenges, and future prospects." International Journal of Communication Systems: e4443.

[14] Ferrag, Mohamed Amine, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. (2017) "Authentication protocols for internet of things: a comprehensive survey." Security and Communication Networks 2017.