An Overview on Security Schemes Based on Elliptic Curve for Cloud-Iot

[1]AMRANI AYOUB, [2]RAFALIA NAJAT, [3]ABOUCHABAKA JAAFAR

[1,2,3]Computer and Telecommunications Research Laboratory, Ibn Tofail Universiy, Kenitra, Morroco

[1]amrani.ayoub@uit.ac.ma, [2]najat.rafalia@uit.ac.ma, [3]abouchabaka@uit.ac.ma

Abstract

The Internet of things appears as a solution in order to connect people around the world. With this concept of interconnection, sharing and dissemination of information between different physical objects. Many objects and services in different fields will be created, such as smart homes, e-health, transport and logistics that will make our everyday needs easier. The main characteristic of a connected object is that it must be identifiable, using technologies such as RFID (Radio-Frequency Identification), must interact with the environment by adding sensory techniques, and finally a connected object must be able to communicate with others. The evolution of Internet of things, increase the number of connected objects. Devices with sensors, generate a huge number of data. With this evolution, the big questions come! how can we control this big data? Cloud Computing a notion that is not newer than the IoT concept, but it's a revolution has steadily been gaining ground. It's a technology that offers to end users a great services in terms of storage, elasticity, analyzing data and other services . In this paper, we cite the benefits of integrating Cloud Computing and Internet of things to manage data provided by physical object and security difficulties that may have this convergence. We also present an overview of the security algorithms proposed in the literature, based on elliptic curves, in order to secure communication between smart objects and cloud computing.

Keywords: Cloud-IoT, Cloud Computing, security, elliptic curve.

Date of Publication: 2018-10-30

ISSN: 2393-9257

Volume: 5 Issue: 01

Journal: *JOURNAL OF ADVANCES IN NATURAL SCIENCES*

Website: https://cirworld.com

How to Cite: Ayoub, A., Najat, R., & Abouchabaka, J. (2018). An Overview on security schemes based on elliptic curve for Cloud-IoT. *JOURNAL OF ADVANCES IN NATURAL SCIENCES*, *5*(1), 352-361. Retrieved from https://cirworld.com/index.php/jns/article/view/7861

1. Introduction

IoT or Internet of things has become a common term in our society, but with a usage that is not very frequent. By 2020 a hundred thousand objects will be connected to the Internet, that communicate and interact with each other in real time without the human intervention. On the other hand, the technology of cloud computing has become very usable. For the general public, cloud computing is materialized in particular by digital data storage and sharing services such as Box, Drop box, Microsoft One Drive or Apple i Cloud, where users can store personal content (photos, videos, music, documents). and access it anywhere in the world from any connected device.

Most of the time, we talk about IoT and cloud computing as two separate concepts. While an enormous amount of data will be generated by smart objects, where to store them and how to manage them? Using the Cloud, mixing it and associating it with the IoT is essential for proper management and use of these objects. Not to mention a vast services that this integration can offer to humanity. Cloud-IoT, new concept can join the wave of new technologies.

In this survey article, we aim at providing a holistic perspective on the Cloud-IoT integration concept and development, including security difficulties for this integration. As a matter of fact, the research community active on Cloud-IoT-related themes is still highly fragmented. We believe that this fragmentation will not help too much the evolution and the development of this new concept. We therefore hoped that this survey will bring together the different axes for collaboration between different researchers in this field. The challenges identified by this paradigm are too numerous, a large community of researchers is needed to fulfil the desired goal.

1.1. Motivation

Due to the rapid evolution of the IoT-Cloud concept. Hundreds of communication between the IoT devices and the cloud, which will transport the data flow, let us say for each user. The informations sent to the cloud via network channels is considered of great importance. Imagine that it's data is not secure enough. Without doubt, this will generate a huge problem and serious consequences. Which will make this Iot-Cloud solution unusable. Security researchers are leaning towards this problem, to secure communication between IoT devices and the Cloud server. There is a few security algorithms which addresses this problem. Our goal in this article, is to make an overview of these algorithms, but only those that are based on elliptic curve. The complexity of this mathematical problem makes the security methods very powerful. This will allow us and other researchers who want to work on this problem, to follow the news of the security algorithms based elliptic curve, and to have a good basis to make contribution.

1.2. Results and Discussion

In this paper, we aim at providing a holistic perspective on the Cloud-IoT integration concept and security algorithms based on elliptic curve. As a matter of fact, the research community active on this themes are still highly fragmented. We believe that this fragmentation will not help too much to develop a good strong algorithm. We therefore hoped that this paper will bring together the different axes for collaboration between different researchers in this field.

The remainder of this article is organized as follows. In Section 2 we define the Cloud-IoT concepts. In Section 3 we will discuss the preliminaries of elliptic curve cryptography. In Section 4 we resume and analyse some works about IoT-Cloud security algorithms based on elliptic curve. In section 5, we will discuss some constraint, and some perspective on current and future works regarding those algorithms, is provided. Finally, section 6 concludes the paper.

2. Cloud-IoT paradigm

An object connected to the Internet, is an object with a certain level of intelligence that can communicate with others based on M2M communication. The birth of the IoT came only for one reason, is to meet our daily needs without the intervention of humans, but with an interaction with its environment by collecting an incalculable number of data, in order to build its own knowledge base. Unfortunately, these objects have an insufficient capacity in terms of storage, energy and robustness. If the data is collected and subsequently deleted due to storage inefficiency, why bring them together? In addition, cloud computing has become mature and can offer storage capacity, robustness and verification, not to mention services for the analysis and processing of data that can be of very great use of objects. An integration between the cloud and IoT will be welcome in order to create a homogeneous environment between the intelligibility of the objects and the robustness of the cloud. Researchers each of them has a vision on how this integration should be [1][2][3]. For me the hypothesis is, why not create a Cloud-IoT environment offering on-demand services for each domain listed in the Internet of things sub-section. As we have already mentioned the cloud is not enough in terms of storage considering the immense demand of the IoT. Recently a new orientation appeared named Fog Computing. According to authors, the Fog is simply a cloud that is close to the ground [4]. The basic principle is to conserve and treat data close to the place of collection. That is to say close to the sensor or the connected object, this will allow us to significantly reduce the flow of data across the network, other benefits are cited in [4]. Despite this Fog will never fill in the functionality of cloud computing [5]. We can say that the cloud and fog Computing complements each other

3. Preliminaries

Before defining the elliptic curves [6], we must put the point on a very important notion, which is the cyclic group. Cyclic group, is a group whose elements are the multiples of a. It's about multiple classics (Z, +) or multiple power (Z, x). The element a is the generator. The order of the group is its number of elements. For example, if $G = \{a^0, a^1, a^3, a^4\}$, next element is a^4 who will be the a^0.

3.1. Introduction to elliptic curve (EC)

An elliptic curve E defined on r is a smooth curve given by a Weierstrass equation:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

We will consider in what follows an elliptic curve, is a curve that is drawn by the points that will solve the following equation:

$$E = (x, y)|y^2 \equiv x^3 + ax + b \; with \; a, b \in K \quad (2)$$

a and b will have to fulfil the following condition $4a^3 + 27b^2 \neq 0$, K can be in the following fields $\{\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}\}$.

Proposition:

Let E be an elliptic curve defined on a field K, and two points P, Q ∈E(K), L the line connecting P to Q (the tangent to E if P = Q) and R the third intersection point of L to E.Let L be the vertical line passing through R. We define P + Q ∈E(K) as the second point of intersection of L' with E. With the law of composition (E (K), +) is an abelian group whose neutral element is the point to infinity (O).

- **Point addition [7]:** With 2 distinct points, P and Q, the addition is defined as the negation of the point resulting from the intersection of the curve, E, and the line defined by the points P and Q, giving the point, R.

P + Q = R → $(x_p, y_p) + (x_q, y_q) = (x_r, y_r) x_r = \lambda^2 - (x_q + y_q)$

$$y_r = \lambda \times (x_p - x_r) - y_p$$

$$with\ \lambda = \frac{(y_p - y_q)}{(x_p - x_q)}$$

- **Point doubling:** When the points P and Q are coincident, the addition is similar, except that there is no straight line defined by P and Q, so the operation is closed using the limit case, the tangent to the curve E, to P and Q. This is calculated as above but with a :

$$\lambda = \frac{(3x_p^2 + a)}{2y_p}$$

- **Vertical point:** The straight line joining any point P and its symmetrical relative to the horizontal axis, noted -P, is a vertical line, the third point of intersection with the curve is the point at infinity (which is its own symmetrical with respect to the abscissa axis), hence P + (-P) = 0.

- **Double-and-add:** The simplest method is the double-and-add method, similar to multiply-and-square in modular exponentiation. The algorithm works as follows: To compute DP, start with the binary representation for$d = d_0 + 2d_1 + 2^2 d_2 + \cdots + 2^m d_m\ \ with\ [d_0 \ldots d_m] \in 0{,}1$.

3.2. Elliptic curve Cryptography (ECC)

3.2.1. What is ECC?

To get started, the RSA keys that have the recommended size, keep increasing to maintain sufficient encryption strength, from 1024 bits to 2048 bits a few years ago, are the most common used for SSL certificates. An alternative to RSA keys are the ECC keys. These two types of master keys share the same important property of being asymmetric algorithms (a key to encrypt and a key to decrypt). However, ECC can offer the same level of encryption power for much shorter keys, providing better security while reducing computing requirements.

3.2.2. What are the differences between RSA and ECC?

The key differentiation between the ECC and RSA is the size of the key compared to the encryption strength.

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Figure 1. Key comparison

3.2.3. Why use it?

The shorter keys make ECC a very attractive option for devices with storage or processing power is limited, which is becoming increasingly common in the era of the Internet of Things. For more traditional Web server use cases, shorter keys can be transcribed into faster SSL negotiations (which can lead to an acceleration of the loading speed of the web pages) and a reinforced security.

3.2.4. **How it works?**

3.2.5. **Example:** Deffiehelman protocol

We will need to understand the notion of scalar multiplication. This group is needed to implement the DH protocol. P is a point that belongs to elliptic curve E.P is a point that belongs to elliptic curve E.

$$P \in E$$
$$K \in \mathbb{Z}$$
$$\mathrm{Q} = \mathrm{KP \text{ with } Q} \in \mathrm{E}$$
$$\mathrm{Q} = \mathrm{P} + \mathrm{P} + \mathrm{P} + \cdots \mathrm{P\,\}\,K\ times}$$

So how do we use this property to create a cryptosystem based on elliptic curves? We need a one-way function. Is a function that can be easily calculated, but that is difficult to reverse - that is, given an image, it is difficult to find an antecedent.

ECDLP: Elliptic Curve Discrete Logarithm Problem

We suppose a curve E($\mathbb{Z}$/n$\mathbb{Z}$). By giving a Q,K ∈ E($\mathbb{Z}$/n$\mathbb{Z}$), with Q a multiple of P. We need to find K that solves the following equation Q = KP. It is a difficult problem to solve. This is called, the discrete logarithm problem or (ECDLP).

Another very important point to know is the point generator.

G ∈ E($\mathbb{Z}$/n$\mathbb{Z}$), which generates a cyclic group.
Ord(G) = n, number of cyclic group element which gives KG = O.
Cofactor: $h = \frac{|\mathrm{E}(\mathbb{Z}/\mathrm{n}\mathbb{Z})|}{n}$, number of points in the curve the ideal is h=1

Let's summarize the parameters we need:

{P, a, b, G, n, h}
p: Field (modulo P)
a,b : Curve parameter E
G: Points generator
n: ORD(G)
h: Cofactor

4. Related works

The security of data generated by the connected objects and transferred to the cloud, requires significant resources such as storage capacity, processing and energy . Unfortunately, the security algorithms used to date to secure these objects. Either they are vulnerable to attack, or they require a huge time of calculation that will eventually exhaust the resources of the objects. We must think of lightweight algorithms, which will respect the object as it is, with its modest resources.

Recently to reduce the computing time for smart device. Schemes based on elliptic curve are implemented. They chose the elliptic curve for many reasons, one of these reasons is its key size which is very small compared to other asymmetric cryptosystems, as shown in Figure 2. Ans also its complexity. Its discrete logarithm is very difficult to calculate.

In 2009 Yang and Chang [8], based on Tian et al's authentication [9], a scheme with mutual authentication and a session key agreement between the user and the server. The server is responsible for initializing the parameters and distributing the public key. This method is very interesting, it does not exhaust the resources of the device, since it is the server that does all the work, but unfortunately this algorithm suffers from the offline password

guessing, and the clock synchronization [10]. In fact, it does not provide all the security necessary for an IoT device. In 2012 Hafizul et al. [11] by demonstrating the vulnerability of Debiao et al's scheme against some cryptographic attacks. He proposed a scheme consists of four steps that we found interesting. Initialisation phase, client registration, mutual authentication with key agreement and finally changing and updating the local private key phase. Unfortunately, again this scheme suffers from the password guessing and does not hide the identity of the client. Other protocols based on ECC have been proposed for smart devices by Granjal et al. [12], Ray et al. [13] and Jiang et al. [14]. Another for IoT using RFID systems always based on ECC, was proposed by Moosavi et al. [15].

Not long ago in 2015, a novel protocol appears, proposed by Kalra and Sood [16], who have gained experience from other previously discussed algorithms. This scheme, is very interesting, they propose a mutual authentication to secure the communication between IoT devices and the cloud using HTTP cookies, for smart device that are HTTP clients. The use of cookies to develop a mutual authentication for smart devices, was very innovative. But in 2017 Kumari et al. [17] after the analysis their scheme, they showed that this algorithm is vulnerable against offline password guessing and insider attack finally this scheme does not provide device anonymity.

4.1. Notes and review of Kumari et al's scheme

Kumari et al's scheme's [17] is one of the last recently proposed algorithms, that secures communication between a smart device and the cloud based on elliptic curves. Until now it seems without weakness, that's why we have chosen to review and leave some notes on this scheme. This method is came, to fix the Kalra and Sood's scheme's [16] to resist the known attacks.

4.1.1. Notion

Table 1.Notions used in this paper

Notation	Description
ID_i	Identity of device i
ED_i	Embedded device
Pw_i	Password of ED_i
CS	Cloud Server
ID_{cs}	Identity of CS
X_{cs}	Secret key of CS based on ECC
Z_p	Finite field group
P	Large prime number of the order $>2^{160}$
r_1, r_2	Random numbers generated for ECC parameters
r_s	Random numbers generated by CS
G	Generator point of a large order n
C_k	Cookie information
E_t	Expiration time of the cookie
h(.)	Cryptographic one-way hash function
$\oplus$	XOR operator
||	Concatenation

4.1.2. Summary of Kumari et al's scheme

The steps followed in this method are summarized in the following figure:

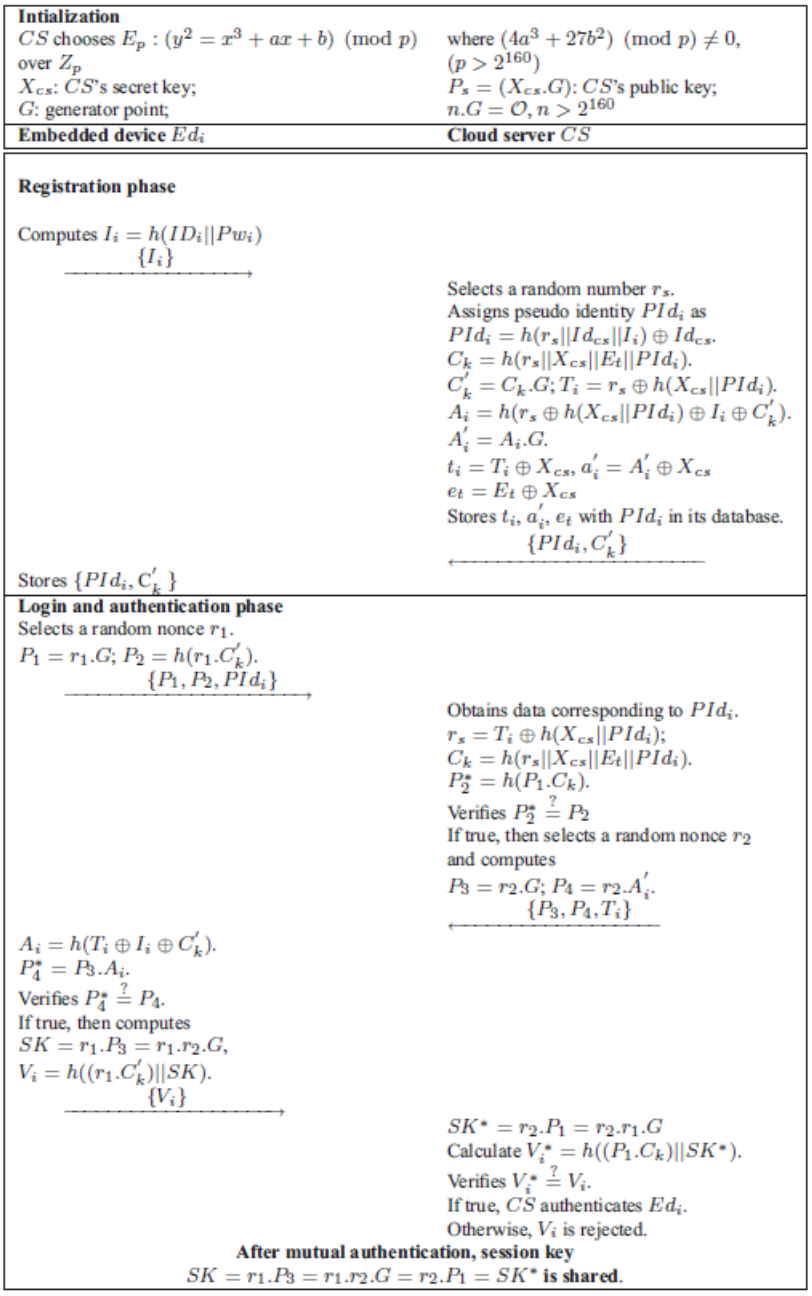

Figure 2. Summary of Kumari et al's scheme

4.1.3. Notes on Kumari et al's scheme

In the initialization step, we do not notice any security flaw, since the choice of the elliptic curve as well as all the parameters, are made in the CS. After this step the cloud server publishes all the public parameters. In the registration phase the Embedded device sends it's Id_i and it's Pw_i hashed to the CS. We notice that Kumari et al. try to keep in safe the identity of the Ed_i, and correct the Kalra and Sood's scheme. After the CS calculate ans stores the cookie information, and the security parameters as shown in the figure 3. The CS sends $\{PId_i, C'_k\}$ to Ed_i, to allow him to login and authenticate. Then, the device computes P_1 and P_2 and

sends $\{P_1, P_2, PId_i\}$ to the CS, who subsequently computes P_2^* and compare it with P_2 sent by the device. If $P_2^* = P_2$, then, CS computes P_3 and P_4 and sends $\{P_3, P_4, T_i\}$ to the Ed_i. Until now no comment, the process is secure. Next the Ed_i computes $A_i = h(T_i \| I_i \| C'_k)$. Imagine that we are hackers, and we have all the public parameters and T_i after a network traffic sniff, also we know the identity of the Ed_i who wants to join the CS. We note that $A_i = h(T_i \| I_i \| C'_k)$ and also equal to $A_i = h(T_i \| h(ID_i \| Pw_i) \| C'_k)$, we think that after an password offline guessing, we could calculate A_i. We think, that Kumari et al. scheme's may be vulnerable to password offline guessing technique, knowing the identity of the Ed_i. The Scheme propose by Kumari et al. is very well done, they left their contribution by correcting some weakness of Kalra and Sood's scheme. But it's still early to confirm the validity of this scheme.

5. Discussion and future directions

IoT-Cloud as we know, is a new technology, to implement it requires a certain level of security. Researchers in this field are trying to find a solution to this problem. In the previous chapter, we tried to summarize some security schemes based on elliptic curve. We found that the majority of these protocols are based on HTTP. Even if the server does the math, the distribution of the keys. We all know that HTTP consumes bandwidth. The mane characteristic of a smart device is its real time responding and interacting with its environment. If we have solved the problem of storage and processing by using the robust capacity of the cloud in order to release smart devices. By using security algorithms that consume bandwidth, and require a lot of computing time, which will exhaust the resource of the device, especially its energy, it's as if the IoT-Cloud solution has come for nothing.

Message Queue Telemetry Transport (MQTT) [18] is a M2M connectivity protocol, designed by IBM as a lightweight publish/subscribe messaging transport . It's a protocol in the OSI model based on TCP/IP and its header size is fixed to two bytes [19]. It's a very interesting protocol, that is suitable for devices which have limited processing. A comparison made in [20], confirms that the use of the MQTT for smart devices consume less bandwidth that HTTP. We believe that this protocol will be a very good solution for devices, until it will be secure. Currently this protocol has some security and intedrity gap. As future direction, we have chosen to focus our next research on how to make the MQTT protocol secure for IoT-Cloud technology.

6. Conclusion

The convergence between IoT and cloud clearly has advantages in several fields, transportation and logistics domain , healthcare domain, smart environment domain and personal ans social domain, especially. In this paper, we tried to define the cloud-IoT concept, expose its advantages. In fact, this convergence is very advantageous, but the issues are very exorbitant. We focused on one of the major problems of this convergence which is security and privacy. After reviewing some known schemes based on elliptic curve. We find that the majority of them are based on HTTP. Things which consume bandwidth and will not be suitable for smart devices. we also discussed Kumari et al's scheme, placing the hypothesis that it may be vulnerable to offline password guessing attack, knowing the identity of the device. Based on comparisons between HTTP and MQTT, we concluded that the use of this protocol will be very suitable for smart devices, thing which encourages us to extend our research to secure the communication between a smart device and Cloud computing.

7. References

1. Alessio Botta, Walter De Donato, Valerio Persico, and Antonio Pescapé. On the integration of cloud computing and internet of things. In Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, pages 23-30. IEEE,2014

2. Stefan Nastic, Sanjin Sehic, Duc-Hung Le, Hong-Linh Truong, and Schahram Dustdar. Provisioning Software-Defined IoT Cloud Systems. pages 288-295. IEEE, August 2014.

3. Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar, and Eui-Nam Huh. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on, pages 414-419. IEEE, 2014.

4. Arslan Munir, Prasanna Kansakar, and Samee U. Khan. IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things. IEEE Consumer Electronics Magazine, 6(3):74–82, July 2017.

5. Manuel Díaz, Cristian Martín, and Bartolomé Rubio. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer Applications, 67: 99-117, May 2016.

6. Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

7. Wikipedia. <https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication>.

8. Jen-Ho Yang and Chin-Chen Chang. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computers & Security, 28(3-4):138–143, May 2009.

9. Xiaojian Tian, D.S. Wong, and R.W. Zhu. Analysis and improvement of an authenticated key exchange protocol for sensor networks. IEEE Communications Letters, 9 (11):970-972: November 2005.]

10. Ding Wang, Ying Mei, Chunguang Ma, and Zhen-shan Cui. Comments on an Advanced Dynamic ID-Based Authentication Scheme for Cloud Computing. In WISM, pages 246–253. Springer, 2012.

11. Sk Hafizul Islam and G. P. Biswas. An improved ID-based client authentication with key agreement scheme on ECC for mobile client-server environments. Theoretical and Applied Informatics, 24(4), January 2012.

12. Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva. End-to-end transport layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In IFIP Networking Conference, 2013, pages 1-9. IEEE, 2013.

13. Sangram Ray and G P. Biswas. Establishment of ECC-based Initial Secrecy Usable for IKE Implementation. July 2012.

14. Rong Jiang, Chengzhe Lai, Jun Luo, Xiaoping Wang, and Hong Wang. EAPBased Group Authentication and Key Agreement Protocol for Machine-Type Communications. International Journal of Distributed Sensor Networks, 9(11):304601, November 2013.

15. Sanaz Rahimi Moosavi, Ethiopia Nigussie, Seppo Virtanen, and Jouni Isoaho. An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems. Procedia Computer Science, 32:198–206, 2014.

16. Sheetal Kalra and Sandeep K. Sood. Secure authentication scheme for IoT and cloud servers. Pervasive and Mobile Computing, 24:210–223, December 2015.

17. Saru Kumari, Marimuthu Karuppiah, Ashok Kumar Das, Xiong Li, Fan Wu, and Neeraj Kumar. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. The Journal of Supercomputing, April 2017.

18. Chyi-Ren Dow, Syuan Cheng, and Shiow-Fen Hwang. A MQTT-based guide and notification service system. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE _th Annual, pages 1–4. IEEE, 2016.

19. Heather Kreger and Jeff Estefan. Navigating the soa open standards landscape around architecture. Joint Paper, The Open Group, OASIS, and OMG, 2009 .

20. Leonard Kleinrock. Queueing systems. Wiley, New York, 1975.