ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-American Journal of Life Sciences and Biotechnology

Vol.10, Issue.2, April 2022

ANOVEL STUDY ON MUTUAL AUTHENTICATION IN Io TUSINGSECU REVAULTS

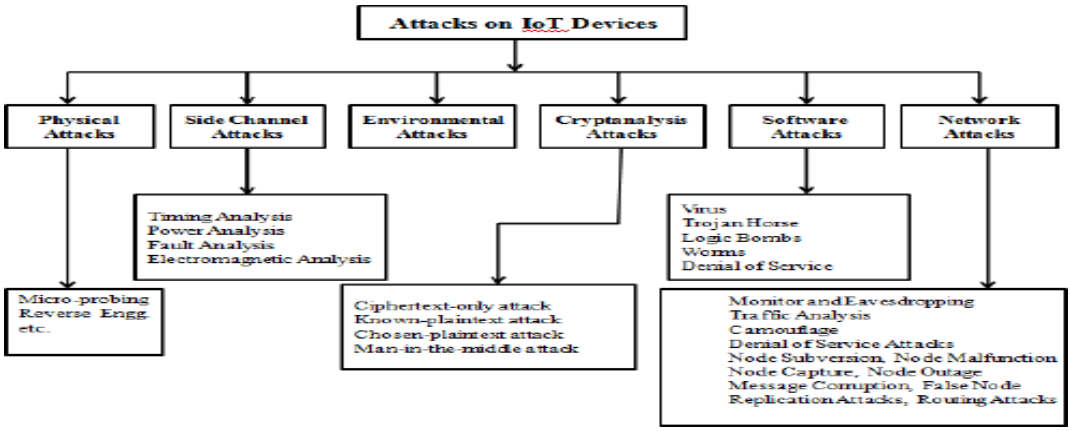
Mrs.AfreenFatimaMohammed1,Dr.AhmedAbdulMoizQyser2

Abstract

Devices that are connected to the Internet can communicate with one other via the Internet of Things (IOT). Fog Server connects every IoT device to the cloud. This data is collected and sent to the cloud by the fog servers, who remove the raw data and only send the bare minimum to the cloud. The data is processed and sent to the cloud server by the fog server. The Fog Server and IoT devices need to be mutually authenticated because authentication is one of the most difficult concerns. Single-password authentications are vulnerable to dictionary and side-channel attacks. It takes a long time to authenticate with biometrics. Secure Vault is the name given to a method of mutual authentication based on multiple keys or passwords that is presented in this paper. Secure Vault is a set of keys with the same thickness. An IoT device and a Fog Server share the Secure Vault contents during the initial stage of communication, and the contents of the Secure Vault change after each session. As a result, side-channel and dictionary attacks are no longer possible.

Keywords—Authentication, Secure Vault, Fog Servers, side-channel assaults, man-in-the-middle dictionary attacks, password prediction, and DoS attacks are all examples of threats that can be mitigated by the use of these technologies.

1. **INTRODUCTION**



2.

1ResearchScholar,CSEDepartmentUCE,OsmaniaUniversity,afreenfatima05@gmail.com
2Professor&HeadofCSEDepartment,MJCET,aamoiz@gmail.com

2. IoT security challenges include authentication, authorization, confidentiality and privacy of data. IoT devices are vulnerable to attacks on the hardware, network, and edge/fog levels. Intruders may be able to access the device's hardware and steal data. It is possible for a "man in the middle" to tamper with data sent from an IoT device to a fog server at the network layer. The Fog Servers, located at the perimeter, are vulnerable to compromise. This means that the Fog Server must be protected by a secure authentication method for the transmission of data from an IoT device. The Fog sits in the middle between the IoT device and cloud architectures. All IoT devices within a short distance of each Fog Server send their data to the Fog Server, which processes it and sends it to the cloud. According to [1], there have been various assaults against IoT devices, as depicted in Figure 1. Cryptographic algorithms are extremely secure. Embedded devices can benefit from algorithms like Elliptic Curve Cyptography (ECC), Advanced Encryption Standard (AES), and RSA. These algorithms are able to run on IoT devices because of their minimal weight. Keys created by these algorithms, on the other hand necessitate safekeeping. How an attacker can get into a device without physically accessing it has been explained in [3,4]. A side-channel attack is the name given to this type of attack. Using side-channel attacks, the AES algorithm's encryption keys can be stolen [5,6].

Figure1.TypesofAttacks

An IoT device is attacked from outside the network by assaults like MIRAI and DDoS Attacks, which get access to the device's user data. Fog servers and IoT devices must be authenticated using an authentication process that is unique to each other. IoT devices and servers can securely authenticate each other using either a public key or a secret key when employing authentication. Side-channel attacks are possible when using a single password for authentication. For this reason, the authors of this study have proposed a multi-key authentication mechanism for IoT devices and Fog Servers. A vault is created by combining a number of keys of the same size. This means that even if an attacker manages to steal a single set of the key, they won't be able to get their hands on all of it. Consequently, the multi-key is referred to as a safe deposit box, or vault. The authentication mechanism is more resistant to side channel attacks when implemented this way. In addition, dictionary attacks can be prevented because the key values change after every session.

3. LITERATUREREVIEW

IoT devices that connect to the network are constantly vulnerable to security risks, such as man-in-the-middle attacks, denial of service and side-channel assaults. An attacker may be able to gain their hands on the device sensors or even the servers itself. You may say that an attacker could take over a sensor and report false data, or the attacker could gain access to a server and mis-activate sensors on its own will. Various network models have been taken into account in the studies according to the goals they were trying to achieve. The clustered network model is one of them. For WSNs in remote IoT applications, [13] discusses a pervasive lightweight authentication system called PAuthKey and a keying mechanism.

Two or more limited nodes or a resource-rich entity must be authenticated before establishing a secure connection. Datagram Transport Layer Security (DTLS) is simplified in the new system (DTLS). ECDSA and ECDH are the main ECC security techniques used in the scheme [12]. Encryption methods have been added to RFID authentication in the context of constrained devices like these. Using the randomized McEliece public-key mechanism[9],

Malek and Miri proposed an authentication method. Untraceability is achieved by this method. A hacker can change the last session such that he/she has a different tag identifier than the one saved in the reader/server. Consequently, the Desynchronizationattack[10] will not be stopped by this protocol. In contrast, the tag uses a circulant matrix during reader authentication, which uses greater processing and storage resources.

It's also not uncommon for networks to use third-party authentication services. Authentication schemes and coexistence proof protocols have been proposed for IoT-based health-care service systems using sensor tags. There is a single sign-on (SSO) authentication method and a coexistence mechanism to confirm the validity of the medical items that exist simultaneously. The trusted third-party authority (TTPAs)[14] helps the users authenticate to the remote server. Kerneesis, a mutual authentication system based on the Needham Schroeder protocol, was proposed in Ceipidor et al. [15]. However, Brute ForceAttacks were a problem with this protocol. In Jan et al. [16], the shared key technique was described. for the server and the IoT device to share a secret key and therefore authenticate each other. Mutual authentication was accomplished through the use of the AES cryptographic algorithm. Two end points must replace their shared keys if this single key is lost or compromised[2].

describes the usage of Elliptic Curve Cryptography (ECC), which was shown to need less memory and processing resources than other public key encryption methods. ECC, on the other hand, necessitates more memory and processing capacity than systems that use a shared key. As stated in [18], ECC is vulnerable to several side channel attacks. IoT device, cloud, and user authentication is covered in Barreto et al. [19] using an SSO-based authentication system. The server communicates with the IoT device after verifying the user's identity through the use of a user credential. Access is granted by the server once authentication has been successfully completed by both end points (the IoT device and the server). In Porambage, et al. [12], an ECC-based two-phase authentication procedure is developed, which is based on the ECC certificate. End-to-end cloud-centric IoT device authentication has been proposed by Butun, et al [20]. To authenticate the user to the IoT device, they employ ECC. ECC-based public certificates or ECC-based Diffie and Hellman key-exchange procedures are used for safe authentication in all of the following mechanisms.

4. MODEL&ASSUMPTIONS

4.1 The network model and underlying assumptions are discussed in detail in this section.

4.2 NETWORKMODEL

On the bottom are IoT devices, on the middle are Fogs, and on the top is a cloud. This network model is represented in Figure 2. There are a number of Fog Servers in each Fog. Connected to each Fog Server is

near-by IoT devices and collects data from them and then forwards the normalized data to the cloud afterremoving abnormalities fromit. An IoT device andFog Servermust authenticate each otherbefore datatransmission.

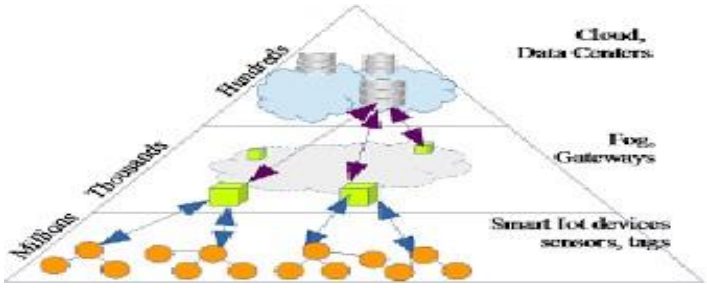


Figure2. NetworkModel ofIoT-Fog-Cloud

4.3 ASSUMPTIONS

In our multi-key authentication approach, each multi-key is referred to as an individual vault. A vault is a set of keys that are all the same size. Considering the security and memory limits, we estimate that an initial vault must include a minimum of n keys, each containing m bits of data. Fog Server and an IoT device share a proposed safe vault at the beginning. Fog Server This paper proposes a three-way mutual authentication scheme for authenticating the Fog Server and an IoTdevice. This scheme uses a Challenge-Response mechanism between an IoT device and Fog Server, which isdescribed asfollows:

Step1:AnIoTdeviceinitiatesacommunicationbysendingaconnectionrequesttotheFogServer.

Step2:FogServerafterreceivingtherequest fromIoTdevice,sendsbackachallengeto theIoTdevice.

5. MULTI-KEYMUTUAL AUTHENTICATIONUSINGSECUREVAULTS

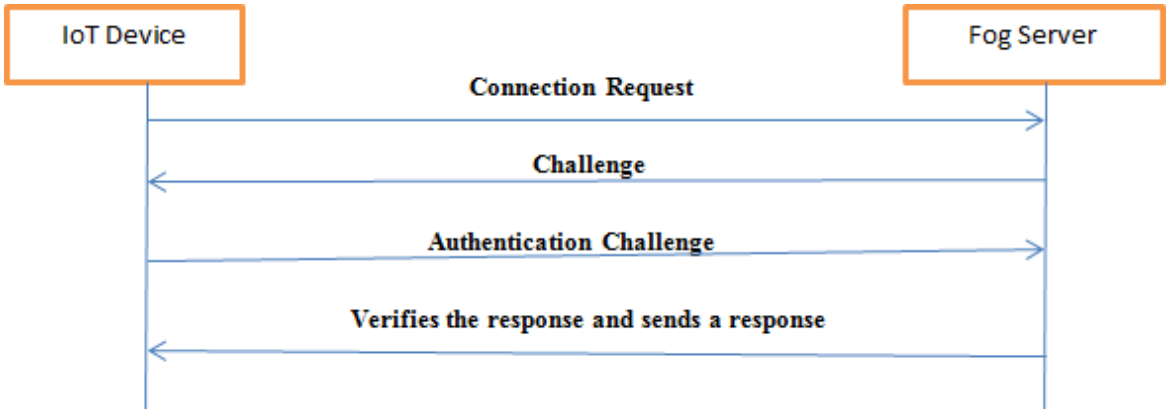
and an IoT device are assumed to have a reliable communication link, so that all messages are transmitted at the same time and there is no data loss. Fog Server is also assumed to have a well protected database and an attacker may be able to exploit Side-channel attacks[2].

4.4 THREE-WAYMUTUALAUTHENTICATIONSCHEME

Step 3:The IoT device responds to the Fog server‟s challenge and sends an authentication challenge to the Fogserver.

Step 4:If the response from the IoT device is genuine, the Fog server checks it and responds back to the challenge.

The Fog server and the IoT device establish a shared secret key, called a session key, during the authentication



5.1 Using a vault of equal-sized n-keys (K[0],K[1],K[2],K[n-1]), the mutual authentication approach employs a secure vault. Each key has a length of m bits. The IoT device and the Fog Server share a secure vault

when they are placed in the network. An IoT device is used to store this encrypted vault. The safe vault is kept in a secure database since we expect that the Fog Server uses a secure database. In the following section, we describe the Challenge-Response Mechanism used in the Multi-Key Mutual Authentication system.

5.2 CHALLENEGE-RESPONSEMECHANIISM

The proposed scheme is a variant of three-way authentication. The notations used in this mechanism is givenbelowinTable I.

TABLEI-NOTATIONS

⊕	Exclusive-OR
||	Concatenation

Followingarethesteps followedforauthenticationofIoTDeviceandFogServer:

Step1: IoT device sends a request message M1 consisting ofDevice ID and a Session ID to the Fog Server,givenas:M1= (Device ID, SessionID)

Step 2: Received by the Fog Server, M1 checks the ID of the registered device that was used for deployment. A Challenge answer C1 and a random number R1 are sent in a message M2 in the event that the Fog Server determines that the challenge is genuine (C1, r1)

Assuming that "p" is a positive integer between 0 and n-1, C1 is the set of "p" distinct numbers; each number represents an index of a key stored in a secure vault. In C1, each digit indicates an index of a secret vaulted key..

Step3:The IoT device responds and challenges Fog Server after getting M2 from Fog Server. It generates the response by conducting an XOR operation on all of the indices stored in C1 to generate a temporary key K1 of "m" bits. It is necessary to use K1 as a common encryption key, which can be generated as follows: K1=K[C11]+K[C12]+C13+.

A random number generated by an IoT device is used to generate a session key, which in turn is used to encrypt (r1 || t1). There is then an additional "p"-differenced challenge C2 that has a collection of "p"-differenced "p"-differenced "p"-differenced "c"-values. Keep in mind that C1 and C2 are not the same. The Fog Server receives a message M3 from an IoT device that includes both a response and a challenge. According to M3, the following information is provided:M3=Enc(K1 , r1 || t1 || (C2, r2)), where r2 is the random number for C2 challenge and t1 is the random number forsessionkeygeneration.

Step 4: When the Fog Server gets the message M3, it generates the key K1 from its secure vault to decode the message received by the IoT device. IoT device can respond to a challenge C2 if the server extracts r1 from a received message. M4 is given by: Enc(K2t1, r2||t2), where k2= K[C21]+K[C22]+K[C23]+. +K[C2p]

The encryption key is K2t1, and the random integer used to generate the session key is t2.

Step5:AfterreceivingM4,IoTdeviceverifiestheidentityoftheserverbygettingbackthevaluer,bydecryptingthemessage M4usingK2⊕t1.

Step6:OncetheFogServerandtheIoTdeviceauthenticateeachother,theydecideonasessionkeyt=t1⊕t2andallthefurthercommunicationforthissessionissecurelyencryptedusingthissessionkey„t".

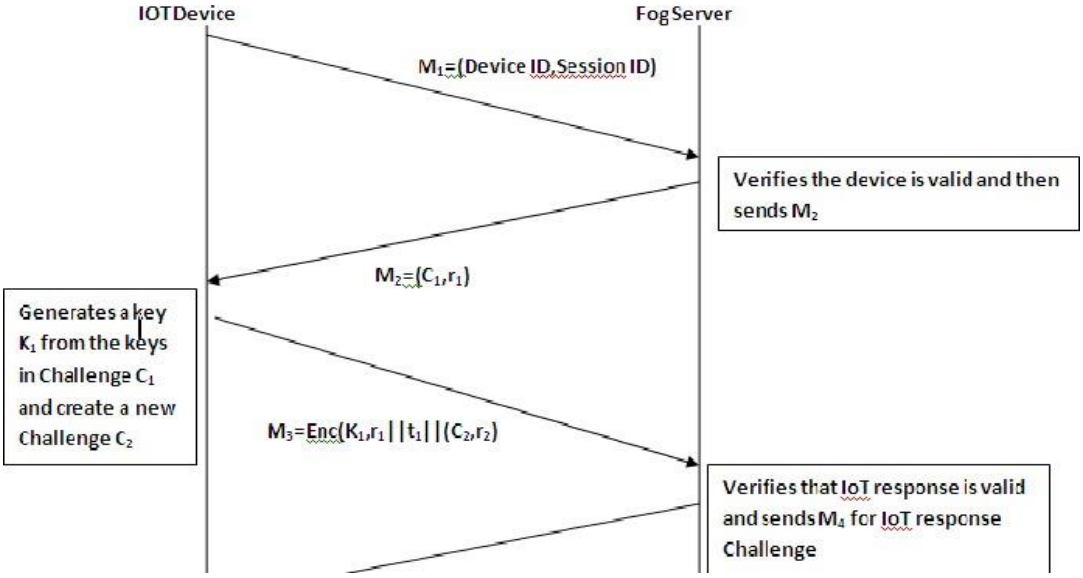


Figure4. ChallengeResponseMechnaism

5

.3 CHANGINGTHESECUREVAULT

The length of the session can be set by the user, if they like. As a result of the shorter length, great security is provided while the 3-way authentication message exchange is rarely invoked. The safe vault's value changes after each session, depending on the information sent back and forth between the server and the IoT device. In order to generate a new value for safe vault, HMAC[7] is used to execute a key-based hashing algorithm on the current value..

5.3.1 **STEPSTOCHANGESECUREVAULT**

Followingarethestepstochangethesecurevault:

Step 1:Using the data transferred between the Fog server and an IoT device as the key for the HMAC, compute the HMAC of the current secure vault. The k-bit output of the hash algorithm HMAC utilized here is „h. Calculating "h" is as simple as the steps outlined below:

h is the Hash Algorithm (HMAC) (current secure vault, data exchanged)

Step 2: A safe vault is partitioned into j equal parts of k-bits, known as vault partitions, which represent the current value. In order to create a new, more secure vault, all of these partitions are XORed together to make the (h I It was found that padding the end of the secure vault with zeroes creates j equal divisions when the vault's size is not divisible by k bits [2].

6. **SECURITYANALYSIS**

Authentication protocol security is under attack from numerous directions. There are a variety of attacks that can be carried out depending on the authentication protocol in use. In this part, we address the attacks examined in [2] in order to demonstrate the security of our authentication process. Man-in-the-middle attacks, next password prediction, side channel assaults, and DoS attacks can all be prevented by the suggested authentication technique. Single-key Authentication and Multi-key Authentication attacks are compared in

TABLE-II.TABLE-IICOMPARISONOFATTACKS

Attack	Single-key Authentication	Multi-keyAuthentication
Maninthe middleattack	✔	**x**

Nextpasswordprediction	✔	**x**
SideChannelAttack	✔	**x**
DoSAttack	✔	**x**

1) Maninthe middleattack

2) To retrieve the session key, the man-in-the-middle will have to use two random numberst1 and t2. There are two random numbers that are sent between the Fog server and IoT device in encrypted communications that use a secure vault that is shared surreptitiously between the Fog server and IoT device. Consequently, a "man in the middle" will have a hard time regaining access to or altering any communications shared between the Fog server and IoT device using the session key.

3) **Nextpasswordprediction**

We show that next password prediction is impossible by an adversary. As it is studied that secure vault changesitscontentsaftereachsessionbasesonthe dataexchangebetweenFogserverandIoTdevice,it isdifficultforanadversarytopredict anyotherpasswordofthenextsecure vault.

4) S**ideChannelAttack**

5) IoT devices are at risk from side channel assaults. If an encryption algorithm like AES[5,6] uses a single key authentication system, an attacker can recover the key and hence break the AES encryption algorithm. It is hard to crack all the encryption keys since the suggested technique uses a multi-key strategy, which uses different keys for each session.

6) **DoSAttack**

With a high number of bogus requests, an attacker may bring down the Fog server or IoT device. Before authentication, no resources are allocated to the Fog Server. Because of this, DoS attacks are ruled out.

7. **CONCLUSION**

The proposed mutual authentication between Fog Server and an IoT device utilizing a secure vault is protected against side-channel attacks. " The contents of the safe vault are constantly updated to prevent side-channel attacks. Secret keys of ongoing authentications can only be obtained by an attacker if the unused authentication keys are also obtained. As a result, side-channel attacks and others of a similar nature are avoided. As a result, a reliable system of reciprocal authentication is provided.

REFERENCES

(1) "Proposed Embedded Security Framework for Internet of Things (IoT)" by Sachin Babar, Antonietta Stango, Neeli Prasad, Jaydip Sen, and Ramjee Prasad, Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark. Bengaluru, India-based Tata Consultancy Services (TCS).

Achieving IoT Device-Server Authentication Through Secure Vaults, 2018 IEEE International Conference on Trust, Security, and Privacy in Computing and Communications/IEE International Conference on Big Data Science and Engineering, Trusit Shah and S. Venkatesan.

Cheap electromagnetic assaults on windowed exponentiation can be used to steal the keys from PCs using a radio. [3] Genkin D., Pachmanov L., Pipman I., and Tromer E. Cryptographic Hardware and Embedded Systems Workshop Proceedings (CHES 2015). From 207 to 228. Springer, 2015.

By using low-bandwidth electromagnetic attacks against PCs, we were able to extract the ECDH key.In the RSA Conference's Cryptographers' Track (CT-RSA 2016).

Published by Springer in 2016, 219–235 Pages

AES TEMPEST attacks by Craig Ramsay and Jasper Lohuis, October 2015.

A.A. Pammu, K.Sc. Chong, W.G Ho, & B.H. (2016, October). Attack on AES-128 wireless communications for Internet of Things (IoT) applications via an interceptive side channel.

IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2016 IEEE Asia Pacific Conference (pp. 650-653). IEEE.
7 Krawczyk, Hugo, Ran Canetti, and Mihir Bhalla.
"HMAC: Message authentication via keyed-hashing." (1997).
[8] Noureddine
IJCNIS, "A Secure Code-Based Authentication Scheme for RFID Systems," Volume 9, Number 1, January 2015, pp. 1-9; FoudilCherif Chikouche A. Miri and B. Malek, "Lightweight mutual RFID authentication," IEEE International Conference on Communications, 2012, pp. 868-872..
[10] NoureddineChikouche, FoudilCherif, Pierre-Louis Cayrel, and Mohamed Benmohammed, “Improved RFIDAuthentication Protocol Based on Randomized McEliece Cryptosystem,” International Journal of NetworkSecurity,17(4),pp.413-422, 2015.
[11] Nan Li, Dongxi Liu, and Surya Nepal, “Lightweight Mutual Authentication for IoT and Its
Applications”,IEEETransactionsonSustainableComputing,, VOL.14, NO.8,AUGUST2015.
[12] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M.Ylianttila,“PAuthKey: A Pervasive AuthenticationProtocol andKey Establishment SchemeforWireless SensorNetworks in DistributedIoTApplications,”InternationalJournalofDistributed SensorNetworks,vol.2014,Article ID357430,14pages,2014.
[13] DaniaQaraBala,SoumyadevMaity,Sanjay KumarJena,”ALightweightRemoteUserAuthenticationProtocol For Smart E-Health Networking Environment”, International conference on I-SMAC (IoT in Social,Mobile,AnalyticsandCloud) (I-SMAC2017).
[14] Hou, J. Li and K. H. Yeh., “Novel authentication schemes for IoT based healthcare systems,” InternationalJournalofDistributedSensor Networks, vol.15, Jan. 2015.
[15] U. B. Ceipidor, C. M. Medaglia, A. Marino, S. Sposato, and A. Moroni, “KerNees A protocol for mutualauthentication between NFC phones and POS terminals for secure payment transactions,” in IEEE Proc. Inter.ISCConf.
onInformationSecurityandCryptology, 2012,pp. 115–120.
[16] Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme forobserving resources in the internet of things environment. In Trust,Security and Privacy in Computing andCommunications(TrustCom),2014IEEE13th InternationalConferenceon(pp.205-211).IEEE.
[17]Kalra, S., &Sood, S. K. (2015). Secure authenticationscheme for IoT and cloud servers. Pervasive andMobileComputing,24, 210-223.
[18] Danger, J. L., Guilley, S., Hoogvorst, P., Murdica, C., &Naccache, D. (2013).A synthesis of side-channelattacksonelliptic curvecryptographyinsmart-cards.JournalofCryptographicEngineering, 3(4),241-265.
[19] Barreto, L., Celesti, A., Villari, M., Fazio, M., &Puliafito, A. (2015, August). An authentication model forIoT clouds.In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social NetworksAnalysisandMining2015(pp.1032-1035).ACM.

[20] Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H.(2016). Cloud-centric multi-level authentication as aservicefor securepublic safetydevice
networks.IEEECommunicationsMagazine,54(4), 47-53.