International Journal of Advanced Technology and Engineering Exploration, Vol 6(58)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2019.650051

Research Article

A new strong user authentication scheme with local certification authority for internet of things based cloud computing services

Youssefi My Abdelkader[1*] and Mouhsen Ahmed[2]
Assistant Professor, Laboratory of Engineering, Industrial Management and Innovation, Faculty of sciences and technologies (FST), Hassan I University, Settat, Morocco[1]
Professor, Laboratory of Engineering, Industrial Management and Innovation, Faculty of sciences and technologies (FST), Hassan I University, Settat, Morocco[2]

Received: 15-July-2019; Revised: 20-September-2019; Accepted: 25-September-2019

Abstract
The term Internet of Things (IoT) refers to the ability to extend network connectivity and computing capability to objects and devices. These devices collect, exchange and analyze data without any human interaction. Generally, IoT architecture requires data communication and cloud computing services. However, security is a big challenge for IoT services. Strong user authentication is the first requirement for IoT services to avoid malicious unauthenticated device. This work explores the weakness of conventional authentication methods in cloud environments. An improved strong user authentication scheme has been proposed. This new scheme is based on local certification authority for IoT devices in cloud computing where devices are authenticated using private public key infrastructure (PKI). The proposed approach has superior security performance compared to conventional techniques. It is shown that our approach doesn't require any hardware tokens, reduce the computation and then improve authentication strength.

Keywords
IoT, Security, VPN, Cloud computing, Authentication, Private key, Public key, Digital signature, PKI, Certification authority.

1.Introduction
In the last few years, the number of connected objects/devices grows, we expect much faster growth in future years. IoT devices are used in different domains: health management, energy management, transportation, smart home, smart cities, agriculture, etc. Traditional internet connects computers or servers to a network. However, Internet of Things (IoT) has a different approach; it connects things to things (device to device) or human to things (human to device). Many enterprises have always trusted only inside users/device to the home network, and managed to share physical resources in the organization. Today, companies also desire strongly to share resources they have stored in their home network devices or outside devices by users everywhere over the internet. Cloud computing is a technology that relies on shared computing resources over a public network, the services are delivered and used over the internet.

The end users ignore the location of physical resources [1, 2]. However, users of cloud have all facilities to manage their applications, with remote access connections. This remote access raises major concerns related to authentication users and/or service provider.

The ability of users to trust IoT services is strongly linked to the level of security ensured by IoT environment. User authentication is the first requirement for cloud services, because cloud data can be accessible to anyone over the internet. This concern has attracted the attention of researchers, and some techniques have been proposed. The first technique used for authentication of remote users was conventional knowledge based on simple login and password, but this way is today insufficient to ensure strong security for important cloud services. This technique requires less effort for attackers to steal login and password [3]. Consequently, strong user authentication techniques improve the strength of

*Author for correspondence

authentication process, compared to login/password techniques.

Strong user authentication approach is the best solution today to secure access to services for cloud-based platforms. Strong user authentication refers to a combination of two or three factors:

- Knowledge of private information such as username and password, code pin, etc.
- Possession of an identification token (piece of data) such as smart card, token, etc.
- Biometric factor (something you are) such as fingerprint, facial recognition, voice recognition, etc.

The strong user authentication is reinforced by the combination of two known and held factors, this combination improves the authentication strength by securing users against theft of private information's [4]. Today, there 'are several methods available to ensure strong user authentication for closed communities with a limited number of employees and partners. These conventional methods involve the deployment of hardware tokens, such as smart cards. However, most of them are not useful for IoT services in cloud environments.

Moreover, these strong user authentication methods are difficult to manage and too costly for cloud computing environment [5].

The objective of this work is to investigate traditional IoT authentication schemes over cloud, evaluate the strength and weakness of existing methods and then propose a new scheme to improve IoT authentication. In this paper, we propose a new solution for strong user authentication, our approach is relatively cost effective to implement for cloud-based services. Our technique is based on local certification authority.

In asymmetric encryption, authentication based on digital certificates ensures authentication using a public/private encryption key. The public key is made available to everyone via a publicly accessible directory or database, but the private key is secret and unique to the device or the user who possesses it. In asymmetric encryption, it is very important to certify the ownership of a public key, that's why an entity called a certification authority (CA) is designed to deliver digital certificates. A digital certificate (DC) certifies the ownership of a public key.

In asymmetric encryption, the authenticity of digital messages is verified using digital signatures. This mathematical process is used to authenticate the sender of messages. A valid digital signature shows to the receiver that the message was transmitted by specific and known user or device. Moreover, valid signature gives the receiver certainty that messages come from authenticated source, and sources of messages can't deny having sent messages [6, 7]. Our strong user authentication scheme is based on digital signature and local certification authority for IoT devices in cloud computing where devices are authenticated using asymmetric encryption. Proposed method improves the authentication strength without any hardware tokens that can be costly and difficult to manage.

This paper is organized as follows. In Section 2, user authentication for IoT services over cloud computing is introduced. Analysis of conventional authentication methods is presented in Section 3. In Section 4, the proposed strong user authentication for IoT services based on local certification authority is presented. Evaluation and comparison are presented in section 5.

2.User authentication for IoT services over cloud computing

Today, most organizations will adopt cloud services, they migrate all or part of their infrastructure to the cloud computing. Moving the infrastructure to the cloud doesn't bring only advantages, it brings its own problems that weren't present in the traditional private infrastructures [8]. Although cloud services have existed in the few past years and a wide majority of companies used it in the daily lives, device authentication is today a serious concern for all companies using IoT cloud services (*Figure 1*).

Authentication is a process through which we can prove and verify the origin of information, the identity of the sender, the identity of a computer or user. Without an efficient authentication rule, we can't manage user access to services, any endpoints can connect to each other without any restrictions. Therefore, it's very important to restrict access, allowing the private network to connect to all of the services of cloud servers, and deny access to unauthorized users. In this article, we discuss several techniques used for cloud services authentication, and we propose an efficient and optimal approach.

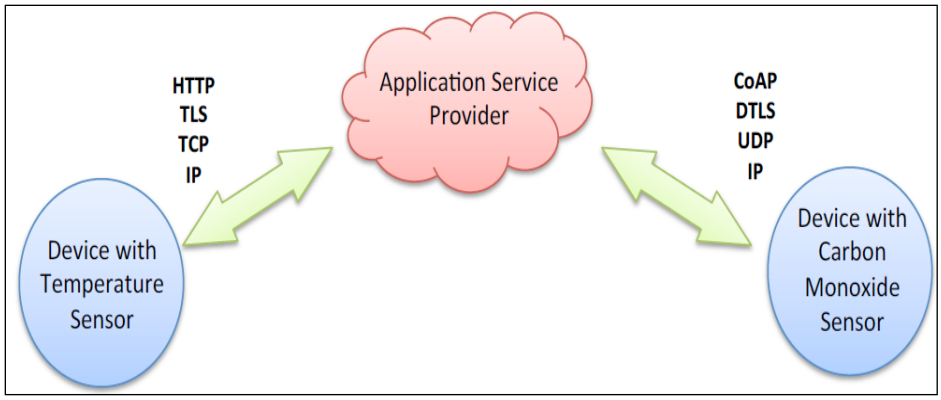

Figure 1 Device communications over cloud computing

3.Analysis of conventional authentication methods

In this section, we present conventional IoT authentication schemes and we investigate their limitations.

3.1Weakness of knowledge-based authentication (KBA)

The first authentication technique used in traditional networks was simple login and password authentication. This conventional method is called knowledge-based authentication (KBA, it is widely used today by web services. KBA requires the knowledge of password and login by the service provider (the authentication server) and the customer (the end user device or the owner of the identity). Therefore, authentication strength is based on knowledge of private information (secret), this secret must be shared between the service provider and the end device user (the customer). This secret is stored in the provider's server This method ensures authentication by comparing the secret given by the customer to the secret stored in the server.

It is technically easy to discover the user's password. Indeed, using tools available on the internet it is quite easy to discover session passwords, brute force attack is the famous attack of knowledge-based authentication. This attack is also known as exhaustive search of passwords [9, 10]. More password is simple, more it will be easy and quick to find out, for complicated passwords, the hacker tries millions of combinations, much time is required to completely reveal passwords. The hacker will need years or hundreds of years to find the complicated password [9, 10]. There are other sophisticated attacks used to steal user passwords quickly and easily, even if the password is long and complicated. Sniffing attacks and man in the middle attacks are widely used by hackers [11]. One-time password (OTP) has been used to replace KBA technique, which is typically weak. Figure 2 shows the login/password authentication process.

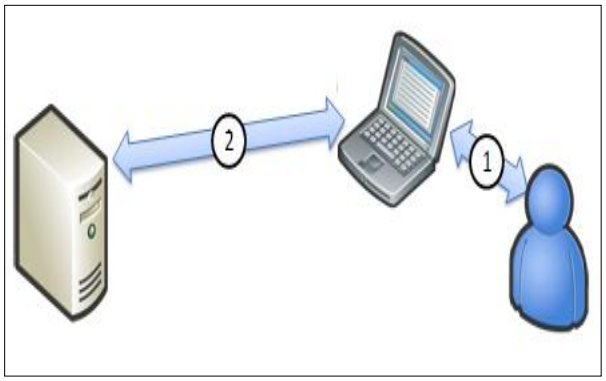

Figure 2 Login/password authentication process

3.2Weakness of conventional one-time passwords (OTP)

With KBA, it is possible for an attacker to replay the same password once it is intercepted. To avoid this vulnerability, we use one-time password to limit password validity. One-time password is valid for one login session. Indeed, for each session or transaction, the user sends a different password generated by an OTP calculator (algorithm). This mechanism requires access to something a person has as well as something that a person knows (such as a PIN).

The same algorithm runs independently on the server side and on the client side. This algorithm provides a new password for single use in the client side, the same password is given by the algorithm in the server side [12]. Figure 3 shows the one-time password process.

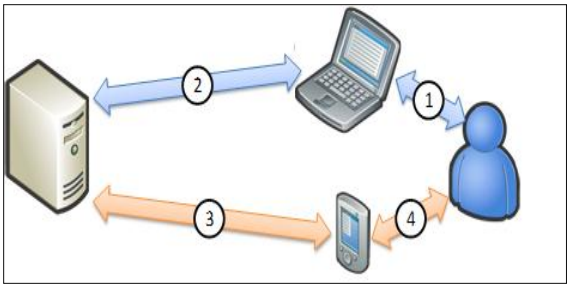

Figure 3 One-time password process

This authentication based on OTP is not vulnerable to replay attacks: even if an OTP is discovered, the attacker will not be able to use this password because it is already used one time to access a service and it is replaced by another secret [13]. OTP technique uses software calculators that are vulnerable, if the user's secret is known, a hacker can download the calculator used by OTP, and then that hacker may generate OTP used for authentication. Moreover, it is possible to steal OTP using passwords brute forcing.

3.3Weakness of conventional strong user authentication in cloud computing

Strong user authentication approach is the best solution today to secure access to services for cloud-based platforms. Strong user authentication refers to a combination of two or three factors:

- Knowledge of private information such as username and password, code pin, etc.
- Possession of an identification token (piece of data) such as smart card, token, etc.
- Biometric factor (something you are) such as fingerprint, facial recognition, voice recognition, etc.

The strong user authentication is reinforced by the combination of two known and held factors, this combination improves the authentication strength by securing users against theft of private information [10]. Today, the ability for an organization to live in the cloud should be included in the security policy. One of the most fundamental elements of this security policy is authentication; access control is needed to verify the identity of devices or users. The implementation of conventional strong user authentication involves the deployment of hardware cards. This technique is useful for closed communities with a limited number of employees and partners. Moreover, these strong user authentication methods are difficult to manage and too costly for IoT devices and cloud computing environment. That's why strong user authentication based on certification authority is today more suitable for cloud computing services because this technique doesn't need any hardware deployment [14].

4.Strong user authentication based on local certification authority

Authentication based on digital certificates ensures authentication using a public/private encryption key. Public keys are made available to everyone by accessible servers or databases, but private keys should be kept hidden in devices.

In asymmetric encryption, it is very important to certify the ownership of a public key, that's why an entity called a certification authority (CA) is designed to deliver digital certificates. A digital certificate (DC) certifies the ownership of a public key (*Figure 4*). This method can also be used to digitally sign transactions and to ensure non repudiation. Digital certificates can be delivered by USB tokens, smart cards or simply by mail. In this section, we will present strong user authentication based digital signature, and then we will present proposed authentication based on local certification authority [15].

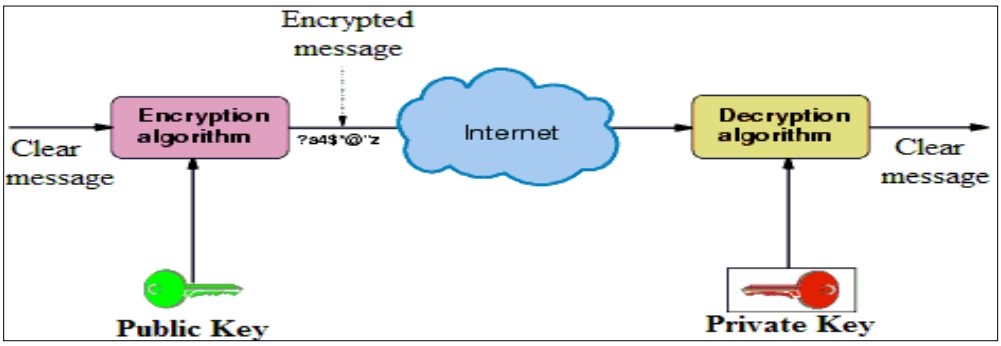

Figure 4 Public key encryption diagram

4.1Strong user authentication based digital signature

The digital signature is used to verify transaction origin or sender [7], it's a mathematical technique used to verify the authenticity and integrity of a message. Digital signatures are based on public key encryption, the steps followed in creating digital signatures are: we first create a hash of the message which will be signed (using a hashing algorithm such as MD-5, SHA-1 or SHA-2), and then the private key is used to encrypt the hash. The encrypted hash is considered as the digital signature of the message. The receiver decrypts the encrypted hash using the sender's public key, and then the receiver can verify the sender's identity and the data integrity (*Figure 5*) [16]. The reason behind the hash encryption instead of the message encryption is related to hashing algorithms, these algorithms are designed to convert an arbitrary small input into a fixed short length value.

The digital signatures use an asymmetric algorithm (such as RSA) that serves as both an encryption and signing technique. While private key used to sign a message is kept hidden, the strength of a digital signature authentication is based on the integrity of public keys: an invalid public key leads to invalid signature. Therefore, the certification authority (CA) is the fundamental element of this authentication technique. All IoT devices/users using digital signatures need to certify the validity of a public key. In the following section, we will present our proposed authentication method based on local certification authority.

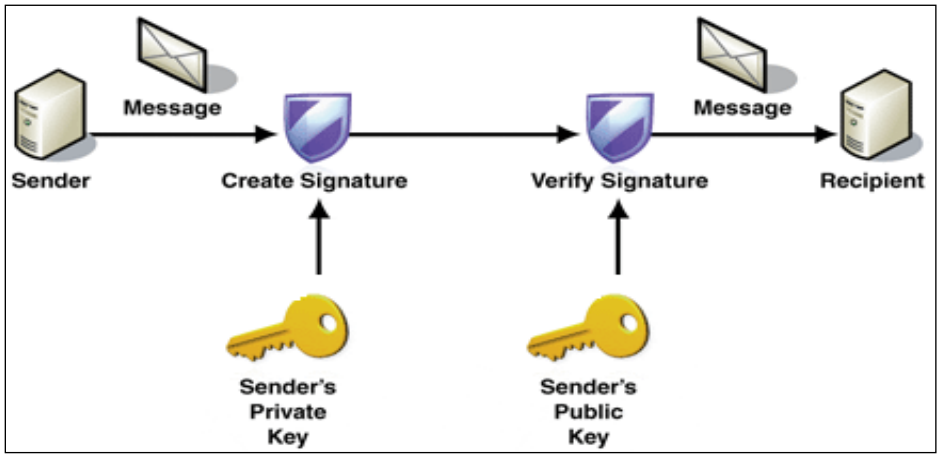

Figure 5 Digital signature process

4.2Proposed strong user authentication based on local certification authority

Today, all public key infrastructures (PKI) are based on digital certificates, the trusted entity that delivers digital certificates is called the certification authority (CA). The CA certifies that a user has a unique public key, in fact, who he claims to have. The CA is an important entity in information security because it ensures that devices/users exchanging data are really who they claim to be. The CA delivers an encrypted digital certificate, including the public key and other identifications (name, address…), the digital certificate (DC) is used to verify device or user identity [16].

Our approach is based on mutual authentication of users using digital certificates (DC). The IoT device and the server authenticate each other through verifying the DC. The CA mutual authentication process between an IoT device and a server involves the following steps (*Figure 6*):

- A device requests access to a server
- The server provides its DC
- The device verifies DC provide by the server
- If server's DC is valid, the device sends its DC to the server
- The server verifies device's DC
- If device's DC is valid, the server allows device's access

In IoT environments, the number of devices grows more and more, traditional CA (single CA) becomes overloaded by the number of DC it has to manage, the companies should control millions of devices: keys generation, validity period of DC, DC revocation, etc. Therefore, in centralized PKIs, long runtime is required to verify or to provide DCs. This limitation is a serious problem because it leaves the

door open for attackers (for example, very slow response to certificate revocation may lead to unauthorized access).

Local certification authority (LCA) is an alternative technique to design fast PKI systems for IoT services. Managed devices are affected to different LCA, each LCA is a geographically disparate entity. Depending on the security policy, different types of LCAs can be created according to geographical location, number or roles of their devices. The functions of these LCAs are subscribing devices and generate DC in a decentralized way.

This approach brings the power of block chain technology to PKIs systems. The LCA method makes the process of certification faster, and then high authenticity and security.

Knowing that for most enterprises with worldwide branches, even if the whole infrastructure is in the cloud, the security of data over the internet is guaranteed with VPN tunnels (IP Sec, SSL,…), authentication is considered for an internal use between enterprise's users, the certification authority is needed only for internal use. Therefore, we can create a local certification authority and avoid purchasing a commercial certificate (*Figure 6*).

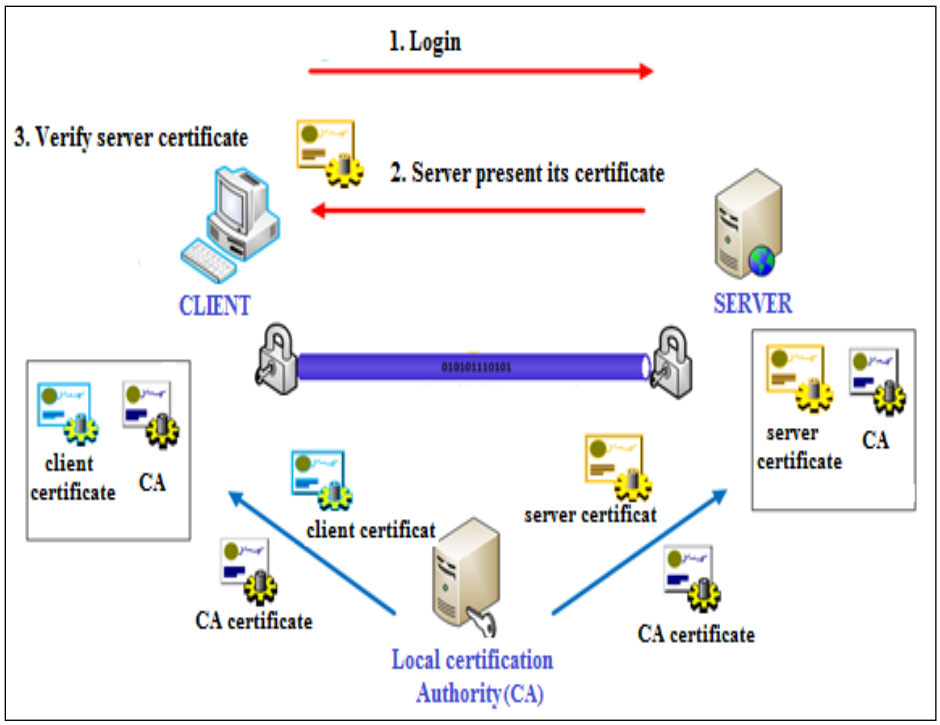

Figure 6 Strong user authentication based on local certification authority (LCA)

Strong user authentication based on local certification authority is proposed to be used for cloud computing services, because of its level of security, its low cost and its simple structure for cloud services. A mutual authentication client/server is used, the client verifies the certificate presented by the server while server verify the certificate presented by the client. In this case certification authority is local because there are a limited number of users and all users are known to the company. This approach shows superior security performance for IoT services compared to conventional techniques.

5.Evaluation and discussion

In this paper, different IoT authentication approaches have been reviewed. The analysis has shown the weakness of traditional authentication methods. For the purpose of comparison, strength and weakness of different methods are shown in Table 1. The methods of authentication based on passwords discussed in section 3, are vulnerable to denial of service (DoS) and man in the middle (MITM) attacks. These types of attacks are widely used by hackers, there are other sophisticated attacks such as sniffing attacks used to steal user passwords quickly and easily, even if the password is long and complicated [17, 18]. In IoT

environments, the number of devices grows more and more, connecting a huge number of IoT devices leads to massive traffic and massive storage. The traditional authentication scheme based on CA (single CA) becomes overloaded by the number of DC it has to manage, and then the computation and the storage cost increase [19]. Our approach based on Local certification authority (LCA) brings the power of blockchain technology to PKIs systems. The LCA method makes the process of certification faster, lower storage, and then high authenticity and security [20, 21].

Table1 Comparison of IoT authentication techniques

Authentication scheme	Token based?	Power of authenticity	Strength (+) Weakness (-)
KBA	No	weak	(+) Computation and storage are low (-) No resistance to DoS attack (-) No resistance to MITM attack
OTP	No	weak	(+) Computation and storage are low (-) No resistance to DoS attack (-) No resistance to MITM attack
Token authentication with CA	Yes	Medium	(+) Resistance to DoS and MITM attacks (-) Require hardware change (-) High storage requirements (-) High computational requirements (slow runtime)
Digital signature with CA	No	Medium	(+) Resistance to DoS and MITM attacks (-) High storage requirements (-) Increase the computation (slow runtime)
Proposed approach based on LCA	No	Strong	(+) Low storage requirements (+) Low computational requirements (fast runtime) (+)Strong ability to prevent different attacks, resistance to DoS attack, MITM attack,

6.Conclusion and future work

The proposed strong user authentication based on local certification authority is specifically tailored to IoT services using cloud computing. The conventional authentication techniques such as KBA and OTP are today insufficient to ensure strong security for important IoT services. These conventional methods are vulnerable to sophisticated attacks on the internet (brute force attacks, sniffing attacks, man in the middle attacks, etc.). Moreover, techniques, implementing conventional strong user authentication using hardware tokens, are useful for closed communities with a limited number of users/devices. These methods are difficult to manage and too costly for IoT services over cloud computing. Our method improves the authentication strength without any hardware tokens and it doesn't require subscription to commercial certificates. In future we would like to propose a low complexity authentication technique for IoT devices in cloud environments.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Hand E. Head in the clouds. Nature News. 2007.
[2] Weiss A. Computing in the clouds. Networker. 2007; 11(4):16-25.
[3] Yang Y, Lu H, Weng J. Multi-user private keyword search for cloud computing. In international conference on cloud computing technology and science 2011 (pp. 264-71). IEEE.
[4] Kaavi J. Strong authentication with mobile phones. Helsinki University of Technology, Fall. 2010.
[5] Jiang R. Advanced secure user authentication framework for cloud computing. International Journal on Smart Sensing & Intelligent Systems. 2013; 6(4):1700-24.
[6] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978; 21(2):120-6.
[7] Kinastowski W. Digital signature as a cloud-based service. In the international conference on cloud computing 2013(pp. 68-72).
[8] Ford M, Stevenson T, Lew HK, Spanier S. Internetworking technologies handbook. Macmillan Publishing Co., Inc.; 1997.
[9] Diffie W, Hellman ME. Special feature exhaustive cryptanalysis of the NBS data encryption standard. Computer. 1977; 10(6):74-84.
[10] Reynard R. Secret code breaker II: a cryptanalyst's handbook. Smith & Daniel; 1997.

[11] Patange T. How to defend yourself against MITM or Man-in-the-middle attack. 2013.
[12] Katz J. Efficient cryptographic protocols preventing" man-in-the-middle" attacks. Columbia University; 2002.
[13] Prakash MV, Infant PA, Shobana SJ. Eliminating vulnerable attacks using one-time password and passtext–analytical study of blended schema. Universal Journal of Computer Science and Engineering Technology. 2010; 1(2):133-40.
[14] Alliance SC. Strong authentication using smart card technology for logical access. A Smart Card Alliance Access Control Council White Paper. 2012:1-26.
[15] Yang B, Hu Z, Xiao Z. Efficient certificateless strong designated verifier signature scheme. In international conference on computational intelligence and security 2009 (pp. 432-6). IEEE.
[16] Tianhuang C, Xiaoguang X. Digital signature in the application of e-commerce security. In international conference on e-health networking digital ecosystems and technologies (EDT) 2010 (pp. 366-9). IEEE.
[17] Atwady Y, Hammoudeh M. A survey on authentication techniques for the internet of things. In proceedings of the international conference on future networks and distributed systems 2017. ACM.
[18] Silva EdOe, Lima WTSd, Ferraz FS, Ribeiro FIdN. Authentication and the Internet of Things: a survey based on a systematic mapping. In proceedings of the international conference on software engineering advances 2017 (pp. 34-40).
[19] Zhou L, Li X, Yeh KH, Su C, Chiu W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Generation Computer Systems. 2019; 91:244-51.
[20] Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Computers & Security. 2018; 78:126-42.
[21] Alizai ZA, Tareen NF, Jadoon I. Improved IoT device authentication scheme using device capability and digital signatures. In international conference on applied and engineering mathematics 2018 (pp. 1-5). IEEE.

My Abdelkader Youssefi was born in Tinghir, Morocco. He received his Engineering degree in Telecommunications from National Institute of Telecommunications (INPT), Rabat, Morocco, in 2003, and he received his Ph.D degree from Mohammadia School of Engineers (EMI) at Mohammed V University in 2015. During September 2003 to May 2016, he was a Telecommunication Engineer. He is now an Assistant Professor in Hassan I University, Settat, Morocco. His research interests include Cognitive Radio, Channel Estimation, Massive MIMO, OFDM and internet of things security in Wireless Networks. He has published more than 15 papers in peer-reviewed journals and referred conference proceedings.
Email: ab.youssefi@gmail.com

Ahmed Mouhsen received his Ph.D degree in Electronics from the University of Bordeaux, France, in 1992, and he is currently a Professorint Electrical Engineering Department, Faculty of Sciences and Technologies, Hassan I University, Settat, Morocco. His research interests focus on Embedded Systems, Wireless Communications and Information Technology. He has published more than 50 papers in peer-reviewed journals and referred conference proceedings.