Authentication Schemes in Internet of Things: A review

Yasmine Labiod
Networks and System Laboratory
Computer Science Department Badji Mokhtar-Annaba University
Annaba, Algeria
yasminelabiod769@gmail.com

Ammara Korba Abdelaziz
Networks and System Laboratory
Computer Science Department Badji Mokhtar-Annaba University
Annaba, Algeria
AMARAKORBA.ABDELAZIZ@gmail.com

Nacira Ghoualmi
Networks and System Laboratory
Computer Science Department Badji Mokhtar-Annaba University
Annaba, Algeria
ghoualmi@yahoo.fr

Mohamed Amine Ferrag
Networks and System Laboratory
Department of Computer Science,
Guelma University
Guelma, Algeria
ferrag.mouhamedamine@univ-guelma.dz

***Abstract*—The Internet of Things also well known as (IoT) has become an important research topic because of its rapid spread and wide deployment in different daily life aspects such as smart home, smart e-health services delivery, smart grid, vehicle connected, government control, etc. Nevertheless, the IoT paradigm raises major security and privacy issues. To secure the IoT devices, many research works have been conducted to countermeasure those issues and discover a better way to remove those risks, or at least reduce their effects on the user's privacy and security requirements. This paper is mainly focusing on critical review of the recent authentication techniques for IoT devices , first we present taxonomy of the current Cryptography-based authentication schemes for IoT. In addition, this is followed by a discussion of the limitations, advantages, Objectives, Countermeasures, and attacks supported of current Cryptography based authentication schemes. Finally, we make in depth study on the most relevant authentication schemes for IoT in the context of users, devices, and architecture that are needed to secure IoT environment and that are needed for improving the IoT security and to be addressed in the future**

Keywords— Security, Authentication, Internet of Things (IoT), Cryptography.

1. INTRODUCTION

The internet of Things (IoT) was first invented by Kevin Ashton in 1999. Internet of Things is an integration of various objects with electronics, software, sensors, and actuators that can communicate directly with one another without human intervention via the Internet to collect and exchange data with each other. The main objectives of the IoT is to fulfill a task in various applications and to achieve a network infrastructure with communication protocols that able to exchange and use information and software to allow the connection and integration of sensors, personal, smart devices, and items, anytime and on any network [1]. Therefore, we can find many applications of IoT in almost all fields. Internet of things is a smart network of different smart objects which can be identified, positioned, tracked, collected and managed remotely.

Security issues, such as authentication, privacy, authorization, Integrity, confidentiality, Encryption, access control, and system configuration are the main challenges in any Internet of Things applications. IoT applications such as Cloud computing, Sensor Nodes, Mobile devices, e-health system can provide a smart environment for global connectivity that facilitates life by being susceptible, adaptive, and reacting to human requirement. However, security is not guaranteed. The authentication is the main regard issue concerning the development of an Internet of Things application and one of the most important and critical requirements for IoT. Traditionally, authentication techniques rely on usernames and passwords, which can be easily compromised and the information on users may be leaked. The main objective of the authentication is to identify users and devices in networks to restrict access to authorized people and non-manipulated objects and to keep information on users protected when user signal is interrupted or intercepted. This issue should be addressed to eliminate the risk, or at least minimize their effects on the user's confidence of personal data and security requirements. Standardization organizations like IEEE and IETF are also working towards making IoT more secure by designing necessary communication technologies. These technologies are important in order to provide mutual authentication between the user and the server, reduce computation and communication overhead in IoT systems, and to make IoT more responsible and power efficient against any attackers.

There are many published surveys on IoT security issues and challenges. Yang et al [2] analyzed existing mechanisms and architectures for authentication, access control, and across-layer techniques whenever applicable. Alaba et al [3] presented a comparative study on IoT security scenario and vulnerabilities. They classified Current IoT security in the context of its application, users, architecture, and communication. Therefore, this paper provides an analysis of the different authentication schemes proposed in the literature. Through an authentication schemes classification, it compares and analyses the existing authentication schemes in the contexts of users, architecture, and devices, and showing their advantages and Limitations. After the introduction, the rest of the paper is organized as follows; section 2 provides the works that are related to

cryptography-based authentication schemes for IoT. Section 3 provides a review of various authentication schemes in the contexts of users. Section 4 provides discussions to the authentication schemes in the contexts of smart devices. Section 6 provides a review of new technologies-based authentication for IoT. Finally, Section 5 concludes the study.

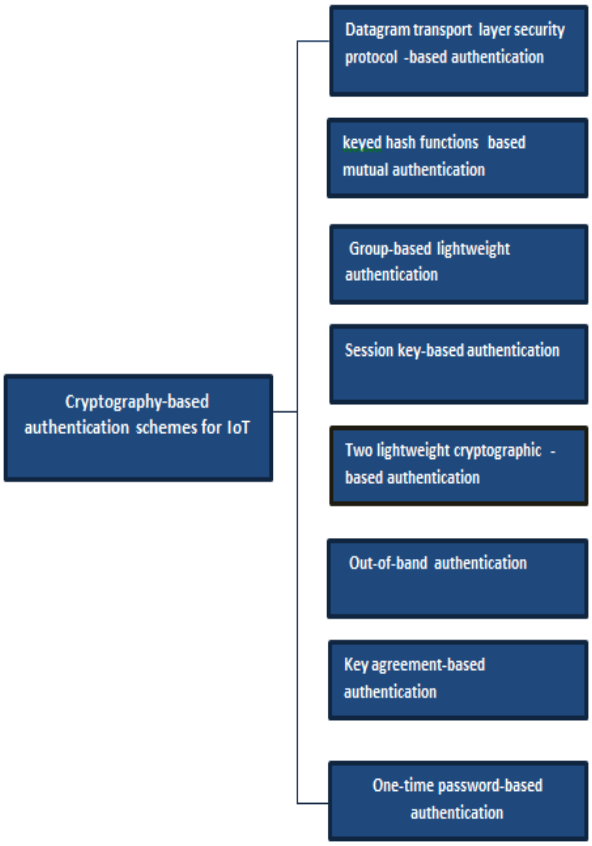

Figure.1: Classification of cryptography-based authentication schemes for IoT

2. Cryptography-Based Authentication Schemes for IoT

2.1. Datagram transport layer security (DTLS) protocol based authentication

Kothmayr et al. [4] proposed the first fully implemented two-way authentication scheme for the IoT system, based on existing Internet standards, specifically the datagram transport layer security (DTLS) protocol. The proposed security scheme is executed over a fully authenticated DTLS handshake and based on the most widely used public key cryptography (RSA) and X.509 certificates. It can work during standard communication stakes that offer UDP /IPv6 networking for 6LOWPANQ. The authors used a low-power hardware platform suitable for the IoT to implemented system architecture.

Perera et al. [5] proposed a pervasive lightweight verification mechanism (the PAuth) for wireless sensor nodes (WSNs) in distributed IoT applications based on DTLS scheme in order to conduct a security analysis on the PAuth Key and measure the security performance of WSNs. They implemented their scheme and demonstrated its performance capacities on the high-resource-constrained sensor nodes. However, many security attacks and issues, such as authentication ,selfish attacks , and multicasting, have been confronted by the distributed IoT due to network heterogeneity, the huge number of resource constraints and device mobility. Hence, an implicit certificate scheme for authentication and large-scale multicasting must be developed, and security protocols that can eliminate the issues of attacks in distributed IoT network applications must be implemented

Authors in [6], presented a two factor authentication security scheme for IoT, by combined existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol and Public key cryptography algorithm (RSA), which is based on the exponential calculation in order to secure data transmission between transport and application layer. This protocol provides secure and efficient authentication for frequent message transmissions in short session time based on the above-mentioned contexts(user, devices, and architecture,) , in addition, they presented the main strength and weakness of this protocol.

2.2. Keyed hash functions based mutual authentication

Moniem et al. [7] introduced an anonymous mutual authentication scheme between RFID server and tagged items for healthcare systems based on keyed hash functions and element extraction. This scheme guarantees the IoT network security and reduces computation and communication overhead in IoT systems. They used this scheme because the RFID tags are constrained in nature, and their computational capability is limited. Anonymity, unlikability, and intractability are the main challenges provided by this mechanism. The simulation analysis shows that the authentication protocol is resistible against anonymity, location privacy threats and tracking attacks such as replay, relay, Dos, and backward security.

Morena et al [8] proposed and designed a two- factor authentication protocol and session key establishment scheme using smart-card for multi-server in distributed IoT application, In order to achieve better smart- card storage cost than others, it based on one- way hash function that is *SHA- 1* ,private key en/decryption technique that is, *AES.* and element extraction. The extracted element is mutually shared with the hash function to evade any jamming attacks. The proposed protocol comprises six phases: initialization phase , registration phase for obtaining cryptographic credentials to the smart- card and end users, login and verification phase, password change, identity change phase and authentication phase for authentication and key establishment in mutual communication. In order to access

many servers, a client (user) needs to register to each server access , all the serve with different login credentials using a single login credential to fulfill their daily needs. The proposed protocol provides a better solution in terms of computation cost , communication cost and it offers the safety features such as session key, user anonymity, efficient login, and strong security protection against all possible attacks such as forgery, off- line password- guessing attacks and Forge reply message attack through formal and informal cryptanalysis.

Amin et al [9] proposed a session key agreement scheme through remote mutual authentication protocol by using mobile application software(MAS) over insecure networks. The proposed protocol based on the non-invertible cryptographic one-way hash function, offered many advantages such as establish a secure connection feature such as mutual authentication, user anonymity, known key secrecy and efficient password change operate, confirm the legitimacy of a user before users can access the resources or services provided by the server , achieve lightweight computation in terms of cost and communication , and avoid the drawbacks of extra cost for maintaining the large number of smart cards and card readers . Ami et al in this scheme proved that the cryptographic one-way hash function is very easy to implement than other cryptographic operations .They cryptanalyzed their scheme in order to prove that is well secured against relevant security active and passive attacks including replay and man-in-the-middle attacks.

2.3. Group-based lightweight authentication

Almulhim et al. [10] proposed a secure group-based lightweight authentication scheme for IoT based E-health applications. The proposed technique creates a session key using on elliptic curve cryptography (ECC) principles. This scheme authenticates IoT devices; builds secure channels among the sensor nodes and the base station (BS), guarantees energy efficient, and reduce the communication cost and computation. The proposed security mechanism is resistible against multiple attacks such as impersonation, man-in-the-middle, and unknown key sharing. The main contribution of [10] is to protect medical data transfer and to exchange data confidentiality in e-health system

The proposed solution in [11] is based on a lightweight key agreement protocol, the Identity Based Encryption (IBE), and Pseudonym Based Encryption (PBE) to ensure anonymity, data secrecy, and trust between IoT or WSN nodes in the network. Their architecture consists of a Base Station BS, a sink node SN, and a set of nodes N. the BS contains the PKG server where the nodes' IDs are stored. Their solution requires architecture consists of a Base Station BS, a sink node SN, and a set of nodes N. the BS contains the PKG server where the nodes' IDs are stored. Their solution requires that all the messages to be transmitted to the SN which then send them to their final destination, and each transmission is acknowledged by an ACK message. The encrypted data will incur a Message Authentication Code function before sending the message. Also, in order to obscure a sent message with an ACK message, the study proposed that both messages will have the same length. Another requirement is that a shared session key should be established between N node and SN, and between SN and BS. Each node N should use a virtual ID and apply PBC technique. Four phases need to be followed to establish the proposed system model. The first step is the network setup, which is also divided in three steps to setup the system's security parameters. These steps consists of configuring the PKG in the BS node, and the SN and N nodes parameters. The second phase highlights the mechanisms that ensures both SN and N nodes are legitimate devices in the network. The third and fourth phase is the establishment of session keys between N node and SN, and between SN and BS. The proposed solution was shown to be resistant to most known attacks in the WSN and IoT. The results also showed an improvement in security and privacy preservative performance

2.4. Session key-based authentication

As the Internet is an insecure channel, it is needed to protect information of communicators. An authentication scheme can fulfill the aforementioned requirements. Recently ,In order to provide two type of authentication mainly: mutual authentication and the session key, Chang et al. [12] proposed an authentication scheme for the IoT. Based on elliptic curve cryptography (ECC), the proposed scheme can enhance the security, and provide a high computational and storage abilities

Maitra et al. [13] proposed a two-factor password authentication scheme based on the hardness assumption of the one-way hash functions and elliptic curve discrete logarithm problem for client-server-based IoT applications. Additionally, by using the proposed scheme, users can easily aware about their wrong inputs in login and password update phases, respectively . This scheme maintains the property of user anonymity as well as dynamic identity so that any adversary will not able to trace a particular user from the communication messages for different sessions between the user and server. Furthermore, security analysis claims that their scheme is free from all possible security threats due to hardness of ECDLP and one-way hash function. They proved that their work prevent all possible attacks and provides the trade-off among storage cost, computational cost, communication cost, and security requirement. The main drawback in their scheme that is based only on theory and no practical proof was presented to support.

Ami et al [14] proposed a lightweight and anonymity preserving three factor user authentication and key agreement protocol for providing file secrecy of the USB mass storage device using cryptographic one-way hash function. Furthermore, They proved that their protocol withstand relevant security aspects of the protocol including

user anonymity, user-server impersonation attack, session key discloser attack and encrypted key discloser attack and they provided the efficacy of their scheme into two phases :login phase and user-friendly password change

phase. After that they analyzed the security of authentication and key distribution protocols using BAN logic, and confirmed that the protocol is completely free from security weaknesses and applicable for practical implementation.

2.5. Two lightweight cryptographic -based authentication

Many devices use the RFID (Radio-Frequency Identification) tags, in order to transfer data to other local or remote devices at various geographical locations and to achieve known security and functionality requirements. This device is vulnerable to many issues as the heavy computational burden and attacks such as replay, forgery, cloning, and DoS. These characteristics pose problematic issues in the application of cryptography protocols to guarantee the IoT network security. For that reason Gope et al. [15] proposed a privacy-preserving radio frequency identification (RFID) authentication scheme for distributed infrastructure with secure localization services for the smart city environment, based on two lightweight cryptographic tools: hash function and symmetric key encryption. This lightweight authentication scheme provides a collaborative security model to reduce the security issues across RFID systems. Also, the main objectives of this scheme are achieving mutual authentication between RFID-tag and backend database server in a distributed IoT system, forward security, achieving strong anonymity, intractability, secure localization, availability, scalability and defeating different attacks. Further, the authors evaluate their scheme for the formal security verification using the AVISPA tool. Two drawbacks in the proposed scheme, first the server can be compromised easily in a DoS attack, which allows an attacker to access and retrieve all available stored information in the constrained medical domains scheme. In addition, the proposed scheme is not securing against physical and cloning attacks.

2.6. Out-of-band authentication

Fu et al. [16] proposed an out-of-band authentication scheme for resource-constrained IoT devices in the context of distributed, cross-domain IoT systems to distinguish the legitimate users from Adversaries. The proposed scheme based on Location-aware approach, cryptographic primitives, it uses the picture taken by the IoT device for authentication by using an out-of-band channel. This approach is usable when the information comes from the unprotected domain to provide a better authentication. The proposed scheme focused on authentication methods to authenticate an unknown object such as Device Compromising Detection methods. In addition, the authors proved that their model is resistible to several attacks such as message replay, deny of service, impersonation, eavesdrop and man-in-the-middle attack.

2.7. Key agreement-based authentication

Wang and Chan in [17] proposed a secure authentication and key agreement scheme for IoT between the embedded devices and the server on IoT network, based on public Key technique such as Elliptic Curve Cryptography (ECC), secure hash algorithm (SHA) and feature extraction in order to consume low computation and memory resources. The technique of key agreement can be merged together with the IoT applications in a variety of scenarios and it further provides effective security. This mechanism makes to prove that the security in Karla and Sood [18] scheme is vulnerable to active attacks. In addition, it makes use of the formal methods to secure communication against different types of attacks.

2.8. Hybrid mutual authentication

Wu et al. [19] proposed an authentication scheme for wireless sensor networks with multi-gateway in IoT environments. Sensor gateways deal with the wireless network and collect information from several distributed WSN nodes. The wireless communication channel implies radio communication, transmitters, and receivers for the data exchange between two or more devices. Therefore, the proposed scheme provides an innovative security which is secure against the simulated attacks and sensor capture attacks. To simulate the security of the proposed scheme, the authors used Proverif tool, as well as evaluating the good performance of the scheme using NS-2 simulation [20]. In addition, the channel is insecure against various attacks.

Amin et al. [21] proposed an anonymous hybrid mutual authentication and key agreement scheme based on preloading of keys and physiological signal function, to protect sensors node in wireless body area network from many attacks such as hub node, impersonation and key escrow attacks. This scheme comprises of four phases: initialization, registration, authentication and key agreement, and master key update. The main objectives of this scheme are to enhance the security and to reduce communication overhead and computational complexity. With BAN logic, the authors illustrated that their scheme achieves security goals and provides secure authentication and key agreement between the sensor node and a hub node and they evaluated that their scheme is safe using AVISPA tool.

2.9. Lightweight authentication

Bose et al. [22] adapted a lightweight authentication scheme for vehicle tracking application based on constrained application protocol (CoAP), in order to secure resource constrained sensor devices, reduce the number of handshaking for reliability, and to secure channel establishment between the sensor gateway and the back-end server. The approach used in this scheme is designed the secure mode of CoAP to be as light as possible, and this method is payload embedded thus minimizing the the handshaking overhead. It consists of four following phases namely: secret distribution; session initiation; server challenge; and sensor response. Two challenges must to be considered in this scheme, the first one is to provide an end-to-end (E2E) application adaptive and ameliorated security

with minimum resource consumption, and the second one is to improve the relationship between the privacy and the security of sensor datasets. The limitation of this scheme that it can only consider a single security scenario (authentication in the connected vehicle).

Al-turjman et al. [23] proposed a lightweight authentication protocol to secure RFID tags. The physical layer of the IoT involves objects, such as RFID and sensors. These objects are restricted in class, and their mathematical capability is limited. These techniques expose a problematic issue to the application of any cryptography algorithms to assure the IoT network. When the RFID is unsafe, a malicious attacker can easily gain access to the network via inspiration and reproducing the electronic product code tag of the victim. The authentication protocol provides a hybrid authentication between RFID readers and tagged items with low computation overhead on the devices

2.10. One-time password-based authentication Baruah et al. [24] proposed a two-factor authentication scheme based on the one-time password (OTP) authentication scheme and physical unclonable Function (PUF), to control, collect information, customize smart home configurations, and to provide enhanced privacy and security via IFTTT recipes. The Internet services (IFTTT) recipes can be changed after just two steps verification process, in the first step, the user has to sign into the IFTTT account and for the second step he has to provide a righteous approval for manipulating the recipe. It further provides an effective security against the FDM attack (Feature-Distributed Malware), Replay, Impersonation, and Tracing attacks.

In addition, it stresses the uses for a few extra resources in terms of storage, computation and communication.

2.11. Lessons learned

The reviewed authentication techniques can be classified according to the following authentication process in two classes : protocol and approach or function, such as : certificate based authentication (CBA), rivest–shamir–adleman(RSA), elliptic-curve cryptography (ECC), datagram transport layer security (DTLS) protocol and different functions/approaches such as one-time password or pin (OTP), Identity Based Encryption (IBE), Distributed Security Management (DSM), on Location-aware approach (LAA) and physical unclonable function (PUF). Table 1 presents this classification. IoT authentication techniques can also be evaluated the performance and demonstrate the completeness of the proposed scheme based on the different tools which is used for automated validation of Internet security sensitive protocols and application The formal security verification plays a critical role in authentication processes. It confirms that the proposed protocols/schemes are safe and secure. In the literature, different authentication approaches used various types of simulator such as AVISPA, NS-2, and Crypto++ benchmark. The majority of the reviewed schemes use AVISPA tool, to demonstrate that the proposed schemes can resist against different attacks.

	Protcol							Functions /approaches						
	CBA	RSA	ECC	DTLS	UDP	CoAP	AES	LAA	PUF	KHF	DSM	OTP	PKG	IBE
[4]	x			x	x	x								
[5]				x										
[6]		x		x										
[7]										x				
[8]							x			x			x	
[9]										x				
[10]			x											
[11]													x	x
[12]			x								x			
[13]			x							x				
[14]	x									x	x			
[15]							x			x				
[16]		x						x						
[17]			x							x			x	
[21]									x				x	x
[22]						x								
[23]										x			x	x
[24]									x			x		

Table1: Authentication Process Classification

In the IoT security domain, establishing an object identity is critical to the privacy and security of the system users and owners. Therefore, authentication is another important security service in the IoT environment. The IoT device credentials must be verified before it can access the PAN resources, further integration of various objects and sensors is vulnerable to anonymity and location privacy threats due to the ID-query replies transmitted from those tags. Authentication includes validation among routing peers of connected IoT objects before exchanging the route information and assure that the source of route information is the connected peer objects, this authentication facilitates enhance the primary element in IoT vision with is M2M communication. There exist many survey articles published [25] during recent years that deal with Internet of Things, focusing on authentication scheme for IoT environments. This work presents a classification of IoT authentication scheme using multiple criteria, which were selected based on the type that we will authenticate and the important features of the existing authentication schemes

Table 1. Summary of different authentication schemes in IoT applications

Scheme	Technologies	Objectives	Countermeasures	System model	Attacks supported	Limitations
Sharaf et al [34]	The Authentication of Devices	To authenticate the objects in the IoT .	Secure Vaults cryptography Protocols	IoT environment.	-Man-in-the middle attacks, and object emulation attacks	Requires hardware change
Barreto etal. [35]	lightweight authentication and keying mechanism	Secure links for end-to-end communication with a strong pervasive authentication mechanism	implicit certificate	IoT applications,	Node compromising attacks, masquerade attacks, and impersonate attacks	Poor flexibility in revoking attribute(time stamp, location identity, or 6LoWPAN identity,)
Lesa et al. [39]	To secure communication between constrained-d IoT	To provide the feasibility, performance, and efficiency	certificates with mutual authentication	IoT SSP Architecture	DoS attacks.	It can only consider a single security scenario
Ramão et al. [42]	Service Oriented Architecture .	To introduce a novel middleware architecture in IoT services	DTLS protocol	IoT middleware system,	DoS attacks.	Minimum latency is difficult to achieve.
Fan and Lin [27]	Three-factor authentication scheme	To provide the privacy of the Biometric data.	Asymmetric and symmetric cryptosystems	Mobile devices	-Replay attacks -Modification attacks	Some attacks are not analyzed such as insider attack
Yeh et al. [28]	Three-factor scheme	To provide mutual authentication between the user and the server.	Elliptic curve cryptography (ECC)	Mobile devices	Insider attacks impersonation attacks de-synchronization attack	Location privacy is not considered
Wu et al. considered [29]	Tree-factor remote authentication scheme	To provides better security	Symmetric algorithms	Mobile devices	Man-in-the-middle attacks, password guessing attacks, stolen verifier attacks	Storage cost is not considered and not resistible against smart card breach attacks
Wang and Wang [30]	Two-factor scheme	To preserve user anonymity	Symmetric algorithms	IoT applications	Smart card breach attacks and stolen verifier attacks	Online/offline dictionary attacks
Zhang et al. [32]	A dynamic privacy protection mechanism	To protect the user's massive private data	hash functions and bio-hash functions	E-health care systems	Sybil attacks	Interest privacy is not
Ami et al [31]	Anonymity preserving remote patient authentication scheme	To preserve user anonymity	Hash function (SHA-1 algorithm)	E-health care systems	online/offline dictionary attacks and man-in-the-middle attacks	Several common attacks

3. User authentication in IoT

In critical applications of IoT (e.g., healthcare and surveillance) real-time data is more needed to gather immediate and corrective actions [26]. Since the sensor gateways deal with the wireless network and collective data information from different WSN nodes, it may not always be real-time. For this reason, we need to design user authentication schemes in IoT in order to access the real-time data straight from the desired sensing nodes.

3.1 Factors-based user authentication in IoT

According to the number of factors considered in a user authentication scheme, it is called a single-factor or a multi-factor scheme. For example, if only the user password is used, a user authentication scheme is called a single-factor scheme. If a smart card (mobile device) and a user password are used, it is called a two-factor scheme, and if the smart card (mobile device), user password and biometrics are used, it is called a three-factor scheme

In order to preserve the privacy of the biometric data of every user, Fan and Lin [27] proposed a three-factor authentication scheme with privacy protection on biometrics using both asymmetric and symmetric cryptosystems, but Yeh et al.[28] found some weaknesses in Fan et al scheme, such as the insider attack and presented a new three-factor scheme based on elliptic curve cryptography (ECC). The main objectives of this scheme are providing privacy of biometric data and achieve the proper mutual authentication between the user and the server. Therefore, Wu et al. [29] showed that Yeh et al 's proposed scheme could not resist the impersonation attacks and the desynchronization attack. Then, they proposed another new three-factor remote authentication scheme. Whereas, this scheme has been ameliorated progressively with efficiency and better security. The cost is always staying not low enough for the mobile devices and the smart chips, which are widely deployed in IoT environments. To remove this problem, many schemes used hash functions algorithm for biometric information (the SHA-1 algorithm) and bio hash functions to enhance the security in different fields such as in e-health systems.

3.2 Anonymity preserving remote user authentication in IoT

In 2014, Wang and Wang [30] pointed out that the two-factor schemes adopting symmetric algorithms failed to preserve user anonymity. Also, they design a conclusion that smart card breach attacks may break the entire system if the verification value is stored in the smart card. They find as a result that they have to use the biometric features to remedy this problem. Therefore, ami et al. [31] showed that Wang and Wang scheme cannot withstand several common attacks, they proposed an anonymity preserving remote patient authentication scheme usable in E-health care systems. Specifically, it makes use of smart card, biometric and hash function (SHA-1 algorithm).

Recently, zhang et al [32] proposed a dynamic privacy protection mechanism for E-health Systems to protect the user's privacy by means of dynamic authentication and three-factor key agreement between the authorized user and the server, which the approach is adding a step of matching biometric features to the scheme. Their scheme is efficient since only hash functions and bio-hash functions are involved. The experimental evaluation shows that the proposed scheme is resistible to several masquerade attacks such as offline password guessing attacks with/without smart cards, de-synchronization attacks and it achieves a number of attractive security features especially privacy protection as Known key security, Perfect forward secrecy, Biometric protection, and User anonymity.

4. Authentication for smart IoT devices

One of the fundamental mechanisms to secure IoT is device authentication. It is useful when two IoT sensing devices need to authenticate each other for secure communications between them. Device authentication provides intruder an opportunity to manipulate the IoT system on a large scale. Authentication and privacy are some of the major security issues of IoT, and it remains a huge issue for IoT devices, which introduces a whole new degree of online privacy concerns for consumers.

4.1 Lightweight acoustic fingerprint-based authentication in IoT

Chen et al [33] proposed a lightweight acoustic fingerprint based on wireless device authentication protocol (named S2M) to provide both low false negative rate and low false positive rate in various scenarios in IoT applications under different attacks.it makes use of the frequency response of a speaker and a microphone from two wireless IoT devices. Therefore, Sharaf et al [34] proposed a new approach for authentication process using the device’s unique fingerprint to compare between security attacks and normal change in fingerprints and to control some characteristics of devices. It adopted the Infinite Gaussian Mixture Model (IGMM), to authenticate devices that have different characteristics spaces offered an authentication mechanism for the IoT environment wherein the devices apply the fingerprinting methods along with the transfer learning. Their scheme is resistible against man-in-the-middle attacks and emulation attacks

4.2. Implicit certificates-based authentication in IoT

Barreto et al. [35] proposed a lightweight authentication and keying protocol based on implicit certificates for Wireless Sensor Networks (WSN) in IoT applications in order to

authenticate the devices, to analyze and deliberate on the security services that can be applied to the IoT devices and to protect the communication between the channel establishments.

Neisse et al. [36] proposed a security toolkit for integrating a management protocol for the IoT devices. The security provides a collection of meta-models and a foundation for developing the IoT security engineering tools. The proposed work aims to address the privacy, data authentication, trust management, and access control requirements for the constrained IoT resources. One drawback of this approach is that the proposed work does not provide a conception analysis on how to spread security and, data authentication solutions for objects operating in a dynamic environment.

4.3. key management scheme -based authentication in IoT

Jang et al. [37] proposed an efficient mutual authentication protocol and key management between all machines –type communication devices based on hash-tree function. Their scheme works without certification authority for the Internet of Things to provide a secure communication and to reduce Computation and complexity compared to the scheme of authentication devices

Sciancalepore et al. [38] presented another device authentication and key management scheme based on public key authentication and Key agreement in IoT devices. Their scheme applies the implicit certificates with public key – based authentication the ECC primitives such as Elliptic curve digital signature algorithm (ECDSA) and elliptic curve deffie-Hellman algorithm (ECDH). It resist against many attacks such replay, DOS, man in the middle attacks, the main objective of this scheme is to provide data authentication ,integrity and secure communication channel environment for confidential data exchange.

5. New technologies-based authentication for IoT

To address the limitations of existing connection-oriented security architecture in terms of the scale and resulting latency on small constrained IoT devices :

Lesa et al. [39] proposed architecture based on certificates with mutual authentication for secure communication between constrained IoT devices using datagram transport layer security.

Moosavi et al. [40] proposed distributed smart e-health gateway architecture to provide data authentication and integrity for IoT-based health-care systems based on public key-based authentication and ECC primitives.

Jebri et al. [41] proposed an architecture based on Identity Based Encryption (IBE), a lightweight key agreement protocol, and pseudonym based Encryption (PBE) to ensure anonymity, data secrecy, and trust between IoT or WSN nodes in the network.

Ramão et al. [42] concentrated on defining a type of classic security architecture for SOA-based IoT middleware systems, which provide the confidentiality, integrity, and protection of communication channels. Support for the heterogeneity and interoperability of IoT devices, information management, and security.

Vucinic et al. [43] proposed object-based security architecture (OSCAR) that influences the security concepts both from content-centric and traditional connection-oriented approaches. They used the secure channels established by means of DTLS for key exchange, and provided a mechanism to protect from replay attacks by coupling with the constrained application protocol (CoAP).

Valdivieso et al.: [44] adopted the SDN architecture in traditional networks, based on encryption methods to control the network and eliminate the rigidity of the network. This architecture makes the network utilization and operation easy by lowering the total cost of organization networks and providing programmable network services.

Gaur et al. [45]: proposed Smart City Architecture based on authentication to facilitate the interaction of distant sensor systems and information.

Vishvakarma et al.[46] :proposed a Lightweight authentication protocol based on key agreement for business community for secure communication between constrained IoT devices and to classify the IoT architectures

Chakrabarty et al. [47]: proposed Black SDN Architecture based on ECC primitives, such as the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie–Hellman (ECDH), to eliminate the issues in traditional IoT systems.

6. Conclusion

IoT Authentication is important to IoT devices, recent attacks show that identification of IoT devices and the authentication done between communicating ones is critical.In this survey, we have presented the security based authentication scheme in IoT applications and systems. We presented the cryptography-based authentication schemes in eight categories; we also studied existing classification of authentication scheme for IoT and security mechanisms to help researchers in comparing and classifying other authentication scheme that, we reviewed the recently proposed IoT user authentication schemes, devices authentication schemes and architectures authentication schemes. Overall, the security of commercial IoT devices today depends on the domain of applications, protocols, and security requirement implemented by each individual manufacturer. Based on the particular phases, all IoT devices could be susceptible to certain types of attacks. This signalizes the urgent needs of developing general security policy and standards for IoT devices and systems.

7. WHAT'S THE FUTURE

In the next three years, even newer security enhancements may be accessible and the system will be up-to-date. The code signing capability with higher encryption levels may be a skip forward to comfy the devices. researchers since this endpoint safety monitoring will see maximum development in the next years. artificial intelligence ,data analysis, machine learning and deep learning will perform an important role in predicting attacks and unsure activity. The contemporary movement towards a mutual IoT standard will have an impact on future security features. The 5G generation could be scalable and speedy enough to help IoT, so that users can be able to obtain enter and to use their home equipment from anywhere without delay. Manufacturing IoT (MIoT) requires remarkably confidential, reliable and fully secure connectivity. Experts believe that 5G provides the perfect platform for IoT. [48]

References

1. Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120–134.
2. Y. Yang, L.Wu, G. Yin, L. Li_, and H. Zhao, A Survey on Security and Privacy Issues in Internet-of-Things Zhao,in IEEE INTERNET OF THINGS JOURNAL,,pp. 2327-4662 , 2016
3. F.A. Alaba, M. O, I.A. T. Hashem, F.Alotaibi, Internet of things Security: A Survey, Journal of Network and Computer Applications, 4 April 2017.
4. T. Kothmayr, C. Schmitt, W. Hu, M. Bryunig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," Ad Hoc Netw., vol. 11, pp. 2710–2723, Nov. 2013.
5. Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. IEEE Communications Surveys and Tutorials, 16(1), 414–454.
6. T. Kothmayr, C. Schmitt, W. Hu, M. Bryunig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," Ad Hoc Netw., vol. 11, pp. 2710–2723, Nov. 2013
7. S.A.Moniem, S.Taha, , and H.S.Hamza†, An Anonymous Mutual Authentication Scheme for Healthcare RFID Systems,IEEE Internet of People and Smart City Innovation journal Department of Information Technology, Cairo University, Egypt,2017
8. T Maitra1, M. S. Obaidat, SK hIslam , D.Giri, and R.l Amin, Security analysis and design of an efficient ECC-based two-factor password authentication scheme, SECURITY AND COMMUNICATION NETWORKS,Security.Comm.Networks(2016) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1596
9. [9]Ruhul Amin,Hafizul Islam,Mohamed Khurram khan , An Efficient Remote Mutual Authentication Scheme Using Smart Mobile Phone Over Insecure Networks,IEEE Transaction
10. M.Almulhim, N. Zaman Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications International Conference on Advanced Communications Technology(ICACT) 2018 February 11 ~ 14, 2018 IEEE,
11. A.Mouhamed,S.Jebri, An efficient scheme for anonymous communication in IoT,IEEE conference paper.
12. C.C.Chang, H.-L. Wu, C.Y. Sun, Secure authentication scheme for IoT and cloud servers, Pervasive and Mobile Computing (2016), PMCJ 665, S1574-1192 00215, 2015
13. Tanmoy Maitra1, Mohammad S. Obaidat2, SK Hafizul Islam 3*, Debasis Giri4 and Ruhul Amin, Security analysis and design of an efficient ECC-based two-factor password authentication scheme, SECURITY AND COMMUNICATION NETWORKS S e c u rit y Comm.networks (2016) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1596
14. Ruhul Amin∗, GP Biswas, Anonymity Preserving Secure Hash Function Based Authentication Scheme for Consumer USB Mass Storage Device, . IEEE Communications Surveys and Tutorials, 16(1), 414–454
15. P.Gope, R..Amin, SK. H. Islam, N.K, K. Bhalla, Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment, Future Generation Computer Systems, S0167-739X(17)31304-3,2017
16. C. Fu, T.Kezmane, X. Du ,Y. Fu, C. reliable authentication scheme for resource constrained IoT devices Morrisseau 2018 International Conference on Computing, Networking and Communications (ICNC): Communications and Information Security Symposium
17. K.H. Wang, C.M. Chen, W. Fang, T.Y. Wu A secure authentication scheme for Internet of Things, Pervasive and Mobile Computing, S1574-1192(16)30436-9, PMCJ 889,2017
18. S. Kalra, S. K. Sood, Secure authentication scheme for IoT and cloud, Pervasive and Mobile Computing 24 (2015) 210 – 223, special Issue on Secure Ubiquitous Computing
19. F.Wu, L Xu, S.Kumari, X. Li, J Shen, K.K.R.Choo, M.Wazid, A. K. Das, An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment, Journal of Network and Computer Applications, S1084-8045(16)30315-0,2016
20. R .kang, The Simulation for Network Mobility Based on NS2, 2008 International Conference on Computer Science and Software Engineering;IEEE explore.
21. R. Amin, G. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Networks 36 (2016) 58–80.
22. Bose, T., Bandyopadhyay, S., Ukil, A., Bhattacharyya, A., and Pal, A. (2015). Why not keep your personal data secure yet private in IoT: Our lightweight approach. Proceedings of the 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), (April), 1–6.
23. Al-turjman, F., and Gunay, M. (2016). CAR Approach for the Internet of Things Approche de la CAR pour l' internet des objets. Canadian Journal of Electrical and Computer Engineering, 39(1), 11–18.
24. B.Baruah, S.Dhal, A Two-Factor Authentication Scheme Against FDM Attack in IFTTTbased Smart Home System, Computers & Security , S0167-4048(18)30240-2,2018
25. M. N. Aman, K.C Chua, and B.Sikdar, A Light-Weight Mutual Authentication Protocol for IoT Systems, Cryptography and Network Security.
26. M. Almulhim, N. Zaman, Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications, International Conference on Advanced Communications Technology(ICACT) ISBN 979-11-88428-01-4 ICACT February 11 ~ 14, 2018
27. S.C. Fan and Y. Lin, Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 4, DECEMBER 2009..

28. H. Yeh, T.H. C.kJ.Hu, W.K. Shih Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data, IET Information Security,2012
29. F. Wu, L.Xu, S.Kumari, X. Li, A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks, Computers and Electrical Engineering, elsevier,2015
30. D. Wang ,P.Wang, Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks, Ad Hoc Networks,elsevier,2014
31. R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, "Cryptanalysis and Enhancement of Anonymity Preserving Remote User Mutual Authentication and Session Key Agreement Scheme for E-Health Care Systems," Journal of Medical Systems, vol. 39,p. 21, Nov
32. Zhang L, Zhang.Y, Tang.S, ,Luo.H , Privacy Protection for E-Health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement, IEEE Transactions on Industrial Electronics, Vol. 65,pp. 2795 – 2805,2018.
33. D.Chen, N. Zhang, Z.Qin, S2M: A Lightweight Acoustic Fingerprints based Wireless Device Authentication Protocol, DOI 10.1109/JIOT.2016.2619679, IEEE Internet of Things Journal
34. Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of things,in 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2016, pp. 1–3
35. Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. IEEE Communications Magazine, 54(4), 47-53.
36. Neisse, R., Steri, G., Fovino, I. N., and Baldini, G. (2015). SecKit: A Model-based Security Toolkit for the Internet of Things.Computers and Security, 54, 60–76
37. S. Jang, D. Lim, J. Kang, I. Joe, An efficient device authentication protocol without certification authority for internet of things, Wirel. Pers. Commun. 91 (4) (2016) 1681–1695.
38. S. Sciancalepore, G. Piro, G. Boggia, G. Bianchi, Public key authentication and key agreement in iot devices with minimal airtime consumption, IEEE Embedded Syst. Lett. 9 (1) (2017) 1–4
39. G. L. dos Santos, V. T. Guimaraes, G. da Cunha Rodrigues, L. Z. Granville, and L. M. R. Tarouco, "A dtls-based security architecture for the internet of things," in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 809–8
40. Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., and Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52(1), 452–459.
41. . Jebri, M. Abid, and A. Bouallegue, "An efficient scheme for anonymous communication in iot," in 2015 11th International Conference on Information Assurance and Security (IAS), Dec 2015, pp. 7–12
42. Ramão Tiago Tiburski, Leonardo Albernaz Amaral, Everton de Matos, and F. H. (2015). T He I Mportance of B Eing, 44(0), 95–128
43. Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., and Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks, 32, 3–16.
44. Valdivieso Caraguay, Á. L., Benito Peral, A., Barona López, L. I., and García Villalba, L. J. (2014). SDN: Evolution andpportunities in the development IoT applications. International Journal of Distributed Sensor Networks, 2014.
45. Gaur, A., Scotney, B., Parr, G., and McClean, S. (2015). Smart city architecture and its applications based on IoT. Procedia Computer Science, 52(1), 1089–1094.
46. [Vishvakarma, N. K., James, W., and R.R.K. Sharma. (2015). Internet of Things Applications - From Research and Innovation to Market Deployment. JIMS, 15(1), 35–43.
47. Chakrabarty, S., Engels, D. W., and Thathapudi, S. (2015). Black SDN for the internet of things. Proceedings - 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2015, 190–198
48. Dongfeng Fang, Security for 5G Mobile Wireless Networks, Utah State University DigitalCommons@USU Electrical and Computer Engineering Faculty Publications.