International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:3, 2018

Comparison of Authentication Methods in Internet of Things Technology

Hafizah Che Hasan, Fateen Nazwa Yusof, Maslina Daud

Abstract**—**Internet of Things (IoT) is a powerful industry system, which end-devices are interconnected and automated, allowing the devices to analyze data and execute actions based on the analysis. The IoT technology leverages the technology of Radio-Frequency Identification (RFID) and Wireless Sensor Network (WSN), including mobile and sensor. These technologies contribute to the evolution of IoT. However, due to more devices are connected each other in the Internet, and data from various sources exchanged between things, confidentiality of the data becomes a major concern. This paper focuses on one of the major challenges in IoT; authentication, in order to preserve data integrity and confidentiality are in place. A few solutions are reviewed based on papers from the last few years. One of the proposed solutions is securing the communication between IoT devices and cloud servers with Elliptic Curve Cryptograhpy (ECC) based mutual authentication protocol. This solution focuses on Hyper Text Transfer Protocol (HTTP) cookies as security parameter. Next proposed solution is using keyed-hash scheme protocol to enable IoT devices to authenticate each other without the presence of a central control server. Another proposed solution uses Physical Unclonable Function (PUF) based mutual authentication protocol. It emphasizes on tamper resistant and resource-efficient technology, which equals a 3-way handshake security protocol.

Keywords**—**Internet of Things, authentication, PUF ECC, keyed hash scheme protocol.

I. Introduction

AS a global network, all components in IoT (including humans and the real world things) have unique identifier, which are used to communicate with each other [4]. Due to the specific features of RFID technology, it is considered as the backbone of IoT since it can solve unique identification problem in IoT [1]. However, the main distinction between RFID and IoT is the presence of sensor. In RFID, an object comes with a tag in RFID so that it is uniquely identified. Meanwhile in IoT, smart objects usually come with both RFID tag and sensor to collect and analyze data.

The term IoT was introduced by Kevin Ashton in 1999, to describe interconnected object in physical world to the Internet [1]. The goal of IoT is to provide smart function in which the processes of gathering meaningful data, analyzing the data and executing actions based on the data are done automatically. Currently, IoT has been implemented in various sectors such as healthcare, water, transportation, energy industry and many others, ensuring faster and better productivity. The example of IoT implementation in healthcare is rural healthcare centre (RHC) system in which registered patients will wear an RFID sensor [5]. If any emergency occurs, RHC doctor will be notified about the situation so that the patient can get proper treatment as soon as possible. Other examples of IoT in different sector are water quality monitoring system and smart meter which will automatically calculate monthly electricity bill.

IoT system involves three layers; a physical perception layer, network layer and application layer [6]. The physical perception layer contains sensors or mobile terminal used for collecting meaningful data in the IoT environment. The network layer is responsible for connecting network devices and processing sensor data. Lastly, the application layer defines various application and delivers specific services to the end-users. However, as IoT technology is advancing, more issues and challenges become apparent to organizations, developers, end-users. In security point of view, data confidentiality and integrity need to be assured. Moreover, the authentication and authorization mechanisms must be applied as well to prevent unauthorized access. Thus, this paper will focus on confidentiality issue with regards on authentication. This paper also provides a few solutions with regards on authentication, either existing implementation or proposed to be implemented in research papers.

The rest of the paper is organized as follows: Section II provides the details on authentication issues including the common authentication method, Section III discusses the proposed solutions for authentication issue as mentioned in Section II; and finally, Section IV is a conclusion for this paper.

II. Challenges

This section discusses and analyzes one of the main issues in IoT security, which is the authentication. In IoT, all components are interconnected in order to produce certain output. While transmitting, the data would be exposed if no security mechanism is implemented. Sensitive data such as the credentials used for authentication can be easily captured during Man-in-The-Middle (MiTM) attack. These highlight the importance of ensuring a secure communication in IoT environment.

Authentication is a process of verifying user's identity, usually based on a username and password. As mentioned previously, without a strong authentication, an attacker may be able to capture sensitive data and execute any unethical action. The problem in IoT system is that, it encompasses billions of devices and they must authenticate themselves to the controller since there is no human operator. Devices in IoT system usually have resource limitation like power and

Hafizah Che Hasan is with the CyberSecurity Malaysia, Malaysia (e-mail: hafizah@cybersecurity.my).

memory making it difficult to apply security techniques based on cryptographic methods with secret keys. But at the same time, authentication is highly important as it conforms user's identity.

A general authentication method in Internet is when websites authenticate users using username and password, while browsers authenticate web sites through the HTTP protocol. From IoT perspective, any social network that connected to a smart object, a link between the online system and the Internet connected device is established by checking the credential using user ID and password to the system [7]. However, communication between the devices and the online server is susceptible to interception from third party intruders, which may lead to data breaches. If using weak passwords policy for Internet-scale authentication is bad, then the implication is worse for IoT-scale authentication. Thus deploying a robust authentication system becomes the first step of providing security and considered as the backbone for any security strategy. It will ensure a much safer browsing experience and online data exchange.

Authorization refers to the rules that allow user to gain specific access or action to system resources based on user privilege. It describes what the user can do which appropriate to that user's identity. For example, a security administrator is able to modify the configuration of application or device while guest can only view the status of the application or device. In information security field, authentication and authorization are two distinct things but related to each other. If the adversary succeeds to bypass any or both security, it may cause a big disaster especially in IoT as many meaningful data can be accessed via the Internet. Not only that, it also affect IoT system performance that can lead to operation failure.

III. Proposed Solution

This section discusses on the proposed solutions for authentication issue as mentioned in Section 2. Proposed solution regarding authentication from various research papers and articles for the last few years were reviewed.

As authentication and authorization are two important security issues of IoT, few solutions had been proposed in order to resolve the issues and reduce the risks. This paper will only focus on 3 proposed solutions for authentication issue; ECC based mutual authentication protocol, keyed hash scheme protocol without Certificate Authority (CA) and PUF based mutual authentication protocol.

A. ECC-Based Mutual Authentication Protocol

Sheetal Kalra *et al* has proposed a secure ECC based mutual authentication protocol for secure communication of embedded devices and cloud servers using HTTP cookies [2]. ECC is a form of public key cryptography which is suitable for constrained environments of embedded or IoT devices that have trusted capability due to low memory and low processing power [2]. It offers better security with smaller key sizes, but at the same times, it ensures higher levels of security compared to other asymmetric techniques. The advantages are more significant for larger key sizes, i.e. a 256-bit symmetric key must be protected by more than 15,000-bit RSA, while an ECC asymmetric key size of only 512 bits provides equivalent security [11].

The prevalence of IoT nowadays has been changed from using hosting websites on dedicated Web servers into scalable cloud-computing clusters for delivering the services. Cloud computing is a type of Internet-based computing that provides a dynamically scalable infrastructure for application, data and file storage on demand.

Cookies are usually used to make web stateful. They help to maintain continuity and states on the web. They usually have been stored on computer's browser directory or program data subfolders. Cookies are designed to provide data specific to a particular client and website for the later server-browser communications. Thus, the web page does not have to ask for the same information repeatedly.

As a cloud server is used to provide service for the smart devices, thus the devices and cloud server must be authenticated each other before it can be employed. Numerous authentication protocols have been proposed or applied for smart devices, but this proposal will focus on the using HTTP cookies for smart device authentication.

The smart device must be configured to act as a HTTP client. Currently, there is specialized software to be deployed for smart devices, which are not having a user interface. This smart device can communicate as HTTP client with a cloud server (HTTP server), which is HTTP enabled. This implies that machine-to-machine (M2M) communication is also possible using the proposed protocol with no human intervention [2].

A protocol proposed by Sheetal Kalra *et al* [2] using ECC approach consists of three phases: registration phase, precomputation and login phase, and authentication phase. Registration phase is where the device need to register with the cloud server before it can be communicated each other. Cloud server will store cookie on the device in order to identify and recognize it.

In the next phase, precomputation and login phase, the device shall connect with the cloud server to send a login request. A mutual authentication through ECC parameter between the device and the cloud server is established upon successful login request sent to the cloud server.

Another approach using ECC based mutual authentication protocol is Secure and Efficient Authentication (SEA). It deploys distributed smart e-Health gateway that is proposed by Sunggyun Jang *et al* [12] that serves as intermediary device. It is also enhanced with data integration and data analysis techniques in this IoT-based healthcare environment.

In this approach, a constrained medical sensor and smart e-health gateway are required to perform mutual authentication through certificate-based Datagram Transport Layer Security (DTLS) handshake between both parties [12]. The sensor and the gateway will initially generate their own private and public keys and exchange their public key. At the final phase of this authentication process, a message will be sent by the sensor to the gateway, in order to verify that it carries the private key that matches the public key stored in the gateway's certificate-

chain. In the proposed architecture, Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) are used for the authentication and key agreement.

The proposed architecture was tested and the result showed that communication overhead and latency are reduced by 26% and 15%, respectively, compared to the current architecture [12]. Although the SEA architecture was tested in the healthcare sector, the ideas and concept of the architecture can be applied to other sectors.

B. Keyed Hash Scheme Protocol without Certification Authority (CA)

Sanaz Rahimi Moosavi *et al* has proposed a keyed-hash based authentication protocol that enables IoT devices to authenticate each other without the presence of a central control server or known as Certification Authority (CA) [13].

Keyed hash scheme protocol uses a secret cryptographic key as input in hashing algorithm. This scheme extends the error detection capability in verifying integrity of data, as well as message authenticity. The most common example of keyed hash scheme is Hash-based Message Authentication Code (HMAC).

In a transmission that using hash function without a key, it only guarantees data integrity. Sender and receiver will generate their own hash using an agreed hash function. Sender will send the hash along with message to the receiver. Receiver then compares its hash with the one from the sender. If match, it means the message has not been tampered. However, unlike HMAC, this transmission cannot establish authenticity.

In HMAC, the presence of a shared secret key helps to establish authenticity since it is generated during a key exchange process that requires the participation of the client and server. Only those two parties know what the secret key is. Thus, they can verify that the message is from legitimate source when the hash is match.

Common authentication protocol in IoT environment involves client (user or sensor node) requests to be authenticated and server notifies that it is ready for authentication process. The client then forms a Message Authentication Code (MAC) data tag using a private key and transmits it to the server. The server will verify the validity of the packet, forms a MAC using the same private key and transmit to the client. The process is finalized after the client verifies the MAC sent by the server. Nevertheless, this protocol is only suitable for heavyweight devices.

IoT devices such as sensor node are limited in resources. They are classified as lightweight or middleweight devices, where the memory size could only be up to 2000 KB, approximately. The suggested key hash protocol only requires device to support minimum 32-bit microprocessor and 512 KB memory size so it is ideal for lightweight devices.

The proposed solution involves each device building a Merkle Hash Tree to produce a Root Hash and use it for authentication purpose. CA is not needed since verification process is done at authenticator device.

The authentication starts when client requests to be authenticated by transmitting an encrypted MAC address or serial number to server. At the server, the encrypted MAC address or serial is divided into leftmost and rightmost value. The rightmost value, known as Time Stamp, is used to build a Hash Tree via four rounds of encryption. The final result is the Root Hash of the server. The server then transmits the encrypted Time Stamp to the client so that the client will produce its own Root Hash, in same way as the server. As output, both client and server will have their own but same value of Root Hash. Finally, the Root Hash is transmitted and authenticated at the server. Once valid, the Hash shake is considered complete.

The competency of the proposed protocol is strengthened when the performance evaluation shows a positive result in the aspect of authentication delay time, code size and power consumption. The comparison is done between the keyed hash, WolfSSL, Constrained Application Protocol (CoAP) and Message Queue Telemetry Transport (MQTT). One of the evaluation is regarding the size of code that is used for authentication process for each platform. The result showed that the code size for keyed hash is only about 4900 KB, making it lightweight and suitable for IoT environment [13].

C. PUF-Based Mutual Authentication Protocol

PUF or also known as object's fingerprint, is a function based on a physical system. The output for this function is arbitrary, making it unpredictable even for an attacker with physical access. PUF was initially built by Pappu [9] by using the random physical variations that can be found in various objects [10].

The authentication solution using PUF is proposed by Muhammad N. Aman *et al* [8] which is to perform PUF based mutual authentication protocol. It is not practical to manage secret keys or cryptographic algorithm in IoT devices because of the limitations in IoT security protocol. On the other hand, PUF circuit is able to obtain secret keys due to the physical features of silicon integrated circuit (IC) instead of storing the keys in the device's memory [3]. For silicon PUF, because of process variations, no two ICs are alike.

In this solution, the secrets keys are embedded into the micro-structure of the PUF IC. Plus, it is not possible to physically tamper the PUF or interfere with the communication between PUF and IC since they are on the same chip. The proposed solution is suitable for constrained IoT devices but servers should not have limitation equivalent to IoT devices. Note that, all encryption and decryption process are done by using XOR operation.

First of all, the server is provided with initial challenge response pair (CRP) before the protocol is run. The next steps of PUF based mutual authentication protocol are simplified as follow:

a) Device 1 (D1) sends its ID_1 & random number, *nonce*
b) Server search for the ID_1 and its respective $CRPs_1$ (Cs_1, Rs_1)
c) Server generates secret random number, N_1 and uses it to encrypt Rs_1. At the same time, server derive Message

Authentication Code (MAC_{S1}) using *nonce* with N_1 as secret

d) Cs_1 and encrypted Rs_1 together with MAC_{S1} is sent to D1
e) D1 generates R_{D1} using its own PUF. $R_{D1\ is}$ then XOR with Cs_1 in order to obtain N_1.
f) D1 derives MAC_{D1} using N_1 and compare MAC_{D1} with MAC_{S1} to verify the integrity of the message
g) D1 generate new secret random number, N_2
h) Next, D1 generates new challenge, C_{D2} using N_1 and N_2 as hashing input. C_{D2} then becomes the input to generate new secret response, R_{D2}
i) D1 also derives MAC_{D2} using N_2 as secret
j) N_2 and R_{D2} are encrypted with N_1 and sent to Server together with ID_1 and MAC_{D2}
k) Server decrypts or calculates N_2 and R_{D2} using its N_1 to obtain its own N_2 and R_{S2}
l) Server derives MAC_{S2} using its calculated N_2 and verify the integrity of the message by comparing MAC_{S2} and MAC_{D2}
m) Server constructs new challenge, C_{S2} using its N_1 and N_2, then stores the new CRP_{S2} (C_{S2}, R_{S2}) against D1 in its memory.

The mutual authentication process is successful after step (l) where server verifies the MAC_{D2}. Authentication fails if any of MAC verification process fails. Other key point of this solution are the CRPs are stored in server's memory while IoT devices only store their ID. After the authentication process is completed, all temporary attributes i.e. secret random number, initial challenge response pair and random number, *nonce* are deleted by IoT devices and server.

Performance analysis done by the authors [8] revealed that the proposed solution requires low processing power, communication overheads and storage requirement. Other concerns in IoT that mentioned in this paper are self-trust, physical and cloning attacks, side channel attacks, MiTM attack and low-cost energy-aware protocols.

IV. Conclusion

One of the main challenges in implementing IoT is authentication. As more organizations are heading towards Industry 4.0, some of them disregard the importance of security aspect in IoT deployment. However, there are some potential authentication scheme can be implemented in order to minimize the attacks and preserve data confidentiality. Fail to do so will result a data to be compromised.

For the authentication and authorization aspect, implementing ECC based mutual authentication, keyed hash scheme protocol without CA or PUF based mutual authentication protocol could be a good help.

There will be an attack to exploit the strength of cryptography algorithm against ECC that has been used. Thus, IoT provider must alert with current attack to ensure that the security in IoT ecosystem is at the optimum level.

The keyed hash scheme protocol without central control will prevent single point of attack but its efficiency is dependent on its cryptographic algorithm during the formation of Hash Tree. Therefore, suitable algorithms that balance between the security and performance, depending on the needs, should be carefully chosen.

The PUF based mutual authentication protocol highlights the unique and tamper-resistant feature of PUFs. However, traditional PUF is analog in nature. Because of its nature, traditional PUF is exposed to analog signal interference in common sensing system. Thus, the suitable PUF should be used to ensure it can extend the functionality of traditional PUF in authentication, un-clonability and verification aspects.

In conclusion, major concern such as authentication and privacy in IoT must be taken into considerations to ensure data confidentiality, integrity and availability. By emphasizing the CIA triad in IoT framework, organizations are more likely to develop, if not, deploy a secure and trusted IoT ecosystem in the new era of Industry 4.0.

References

[1] Mete Akgün, M. Ufuk Çaglayan, Providing destructive privacy and scalability in RFID systems using PUFs. Ad Hoc Networks 32 (2015) 32–42
[2] Sheetal Kalra, Sandeep K. Sood. Secure authentication scheme for IoT and cloud servers. Pervasive and Mobile Computing 24 (2015) 210–223
[3] SS kumar, J guajardo, Rmaes, GJ schrijen and P tuyls, The Butterfly PUF: Protecting IP on Every FPGA, in: Proceedings of the IEEE international workshop on hardware-oriented security and trust, 2008, pp. 67–70
[4] R. Aggarwal, M.L. Das, RFID security in the context of internet of things, in: Proceedings of the First International Conference on Security of Internet of Things, SecurIT '12, ACM, New York, NY, USA, 2012, pp. 51–56.
[5] Vandana M.R., Neeli R.P. and Ramjee P. (2011). A Cooperative Internet of Thing (IoT) for Rural Healthcare Monitoring and Control, (Aalborg University Denmark).
[6] Zheng Yan., Peng Zhang, Athanasios V. Vasilakos. (2014). A Survey on Trust Management for Internet of Things, pp. 120-134.
[7] Tuhin Borgohain, Amardeep Borgohain, Uday Kumar, Sugata Sanyal. Authentication Systems in Internet of Things.] R. Aggarwal, M.L. Das, RFID security in the context of internet of things, in: Proceedings of the First International Conference on Security of Internet of Things, SecurIT '12, ACM, New York, NY, USA, 2012, pp. 51–56.
[8] Muhammad N. Aman, Kee Chaing Chua, Biplab Sikdar, Physical Unclonable Function for IoT Security, in: IoTPTS 2016 Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 10.13 http://dx.doi.org/10.1145/2899007.2899013
[9] P.S. Ravikanth, Physical One-Way Functions, Ph.D. thesis, Massachusetts Institute of Technology, 2001.
[10] F. Armknecht, R. Maes, A. Sadeghi, O.-X. Standaert, C. Wachsmann, A formalization of the security features of physical functions, in: 2011 IEEE Symposium on Security and Privacy (SP), 2011, pp. 397–412. http://dx.doi.org/10.1109/SP.2011.10.
[11] K. Imamoto, K. Sakurai, Design and analysis of Diffie–Hellman based key exchange using one-time ID by SVO logic, Electron. Notes Theor. Comput. Sci. 135 (2005) pp. 79–94.
[12] Sunggyun Jang, Ducsun Lim, Jinyeong Kang, Inwhee, An efficient device authentication protocol without Certification Authority for Internet of Things, in: Wireless Pers Commun, 2016, DOI 10.1007/s11277-016-3355-0.
[13] Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen, SEA: A Secure and Efficient Authentication and Authorization architecture for IoT-based healthcare using smart gateways, in: Procedia Computer Science 52 (2015) 452 – 459, http://dx.doi.org/10.1016/j.procs.2015.05.013