International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 30337-30344
© Research India Publications
http://www.ripublication.com

# A Security Framework For Internet Of Things (Iot) Authentication Using Certificates

**T B Stanley[1], S Murali Krishnan[2], P Prakash[3]**
*[1,3]Department of CSE, Amrita VishwaVidyapeetham, Coimbatore, India.*
*[2]Honeywell Technology Solutions, Bangalore, India.*
*[1]stanley1191@gmail.com, [2]muralikrishnan1990@gmail.com, [3]npprakash@gmail.com*

## Abstract

As more number of devices are connected to internet day by day, directly or indirectly for different needs like monitoring, management, automation and so on. Number of devices connected to internet is more than the number of people connected to it. Among the devices that are connected to the internet, most of the devices are used for communication and collection of data in real time. Providing security for devices over the internet is becoming challenging task since data processing is in real time. In this paper, we introduce a new cost effective framework using a private Certificate Authority (CA) to detect these rogue devices trying to connect to the web server and then to prevent them from connecting to the web server. We use MAC address with certificates for authenticating a device. Our proposed security framework improves the security by detecting and preventing the rouge devices in Internet of Things (IoT). Most number of attacks are reduced by identifying and restricting the rouge devices in the network.

**Keywords:** IoT; Certificate; CA; rogue; cost; authentication; security.

## Introduction

Internet of Things (IoT) is the physical things like sensors, surveillance cameras, coffee machines etc. connected through internet, which is introduced in 1999 [1]. IoT becomes mandatory in almost all systems like automations, monitoring systems and so on. These devices collect and share the data over the internet. Each device is connected to internet with unique address for unique identification. Heterogeneity, mobility, interoperability, distributed these all are the basic properties of IoT. Since these devices have the information related to state of environment, private details, security is more important for IoT [2].

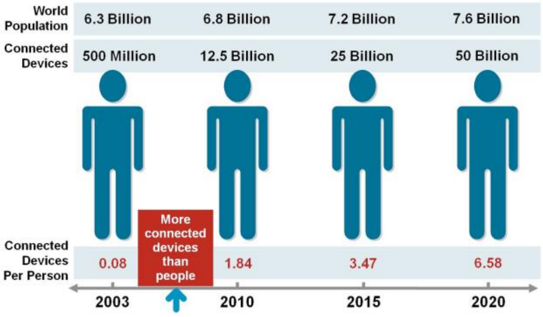

**Figure 1:** IoT forecast(source: Cisco IBSG, https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf)

As shown in figure 1, number of IoT devices are getting increased exponentially over the years [3].

There are more opportunities for attackers in IoT, since all the devices are connected through internet and the internet is open to everyone. Security in IoT includes securing information, restricting unauthorized access to the device and providing confidentiality of data. We are proposing framework for security in IoT which is using MAC address and certificate to authenticate.

The IoT can be broadly classified into two categories. They are Industrial IoT and Commercial IoT. In this paper we will be focusing more on the Industrial IoT.

**Industrial IoT:** In this type of IoT all the data from the devices should be tracked for the security of the organization and also to analyze the data for better decision making in the organization. In order to achieve this all the devices should be connected to a server. So all the communication takes place through the server. This is a centralized model [4].

**Commercial IoT:** In this type of IoT there is no need to track the data from the devices. So the devices can communicate directly with each other using Bluetooth, ZigBee etc without connecting to a server. This is a distributed model.

Do we really need to authenticate the devices in the IoT? Well, when a device is used inside an organization we definitely need the devices to be authenticated because attackers may tamper a device in the organization and add some malicious code into it so that it changes its behavior and also if an attacker tries to add a new device to the present devices it should not be given access. So in this paper we will be discussing the solution for this problem.

Section II contains the related work done, III deals with proposed security framework architecture, section IV explains the implementation modules of our proposed framework and the final conclusion of this article added in section V.

## Related Work

Network security becomes more important for IoT devices since all the devices are connected with internet. More number of attacks are possible against confidentiality, integrity, availability and authenticity of devices when it is connected through internet.

There has been lot of challenges in providing security over IoT devices. We discussed some of the proposed methods in providing security over IoT device as follow.

Liang Zhou, Chao H [5] proposed a Media-aware Traffic Security Architecture (MTSA) for IoT devices and they proposed a method to classify the traffic is scalable or not. MTSA is an improved architecture of existing information security architecture. It adds multimedia traffic and contents to existing information security architecture. MTSA provides security based on the traffic needs. Dong Chen [6] proposed a novel security architecture which comprises of four layers as intelligent service layer, data perception layer, heterogeneous network access layer and data management layer for IoT devices. They also discussed the security requirements for the IoT devices in each layer.

Kai Fischer [7] analyzed and introduced new security architecture elements for plug and work of devices. They focused on security elements like service device identifier, secure credential management; secure network access of devices and device and system integrity assurance. Xiong Li [8] proposed a general architecture of trusted security system based on IoT. The trusted security system architecture is realized with modules of trusted user, trusted perception, trusted terminal, trusted network and trusted agent. Habtamu Abie [9] proposed a risk based adaptive security framework for smart IoT devices in eHealth. The framework uses game theory and context awareness techniques to predict and estimate the risk damages and future benefits. Antonio J. Jara [10] proposed an architecture which supports mobility and security for IoT devices in medical environments. Security between devices is provided with help of Near Field Communication (NFC) medical devices which is equipped with cryptographic SIM card. Handover process time is reduced by neglecting the addressing stages for better mobility with respect to 6LoWPAN (IPv6 over Low power Wireless Personal Area Network).

### *A. Detecting Rogue devices*

Most of the attacks are prevented by detecting rogue devices in IoT. Rogue devices are unauthorized devices in the network which causes significant risk to organizations. We discussed some of the existing methods for authenticating the devices in IoT and its drawbacks.

#### *1) Password based authentication*

Passwords are used to authenticate and gain the access of devices in IoT. Passwords are already stored in a database of the server so that authentication done with help of password match. If the database containing passwords is compromised then all the devices become vulnerable to the attacker.

#### *2) MAC address based authentication*

Every IoT device is manufactured and assigned with unique address of 48 bits which is known as MAC address. Since MAC address is unique, MAC filters are used to restrict the rogue devices in IoT. Drawback of the technique is intruder in the middle can spoof the MAC address of a device and can gain access over the data [11].

*3) Commercial Certificates*

The commercial certificates provide trust for the devices, so the device certificates can be verified by public servers because they already have the public key in their trust store. These certificates are issued by trusted Certificate Authorities like Symantec, Thawte, Comodo etc. but the drawback is that these certificates are expensive. As the number of devices are increasing in the Internet day by day it is not a good idea to pay for certificates for each device.

*4) Self signed Certificates*

Self signed certificates can be generated easily with the help of tools like OpenSSL library, Java toolkit etc. The advantages of these certificates are zero cost, generate rapidly and are easily customizable. These certificates can be used in place of commercial certificates. Both give the same level of security but the problem is these certificates cannot be trusted by other users as the Certificate Authority who issued this certificate is not trusted. But this may work well in case of devices in an organization.

## Proposed Framework

Our proposed system is designed as shown in figure 2. It uses MAC address with certificates to authenticate the devices uniquely. Our proposed system includes Private Certificate Authority, manufacturing unit, server, clients and devices as main elements. There are two types of clients wants to access the devices data, they are through web clients and mobile clients. All clients can access the data from the devices through central server. The Web Server contains an authentication server which helps to authenticate each device uniquely by using certificates. All the devices are connected to authentication server through Secure Socket Layer (SSL) connection to avoid intruders. Each device sends its unique identifier (MAC address) and public key to the manufacturing unit to build a device specific certificate. Private Key of Private Certificate Authority is used to sign these device certificates. These devices certificates are then send to each device from manufacturing unit. The public key of Private Certificate Authority is loaded to the trust store of the authentication server to verify the device specific certificates. Authentication server decides the device is not a rogue device depends on below conditions.

- If the certificate is valid then the device is not a rogue device.
- If the certificate is invalid then the device is considered a rogue device.

When the device is authenticated as not a rogue device, a SSL connection is established between authentication server and device. Using this SSL connection the data is transferred between the server and the device. The data will be sent in a fixed size segments. These data segments will be signed using the private key of the device and the server on the other side can verify the signature using the public key of the device. By doing this we are providing integrity to the data sent from the device and increasing the overall security of the device.

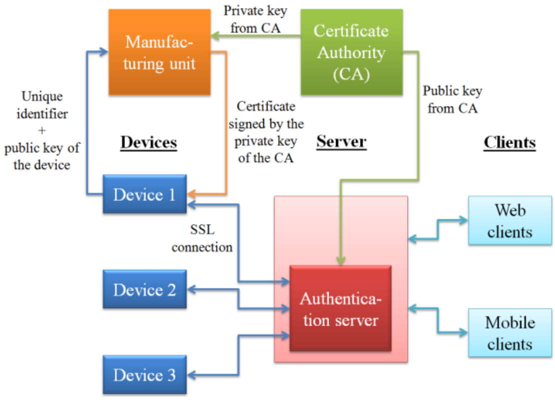

**Figure 2:** Proposed Security Framework

*B. Advantages of our proposed system*

*Device specific certificates:*
Device specific certificates are more secure than giving common certificate for all devices. Each device specific certificate contains the information related to the particular device. So if a device is compromised still the other devices are secure. So there is no centralized failure of the whole system [12, 13].

*Low or Zero cost certificates:*
Our proposed framework authenticates the devices with very low or zero cost certificates by using its own Private Certificate Authority rather than Trusted Certificate Authority. Commercial certificates are very expensive to use as number of devices increases.

*Spoofing of certificate is avoided:*
Spoofing of certificate is avoided by making the device firmware tamper proof by encrypting the firmware and also digitally signing the firmware. If a certificate is retrieved from the firmware it cannot be used for another device because each certificate contains the information of a particular device. So spoofing becomes extremely difficult.

## Implementation

In the implementation part we tested on the system in Windows environment using OpenSSL in Cygwin. The certificates we used in for this demonstration is in the X.509 format. First the thing we need to do is create a Private Certificate Authority, for that we need to create a public and private key pair and create a root certificate which is self signed i.e. signed by its own private key. This root certificate is then used to verify the device specific certificates. As we know each device have a unique MAC address this MAC address is used by the device to generate the certificate request. To generate the certificate request we need the private key and the MAC address. This certificate request is then sent to the Manufacturing unit. This production infrastructure verifies the certificate request sent by the device and then signs the device specific certificate with the private key of the Private Certificate Authority. Then these device specific certificates are sent back to the devices. Each certificate will contain the MAC address of the particular device as the common name in the device specific certificates which is used to identify the device uniquely. Now when a device needs to send data to the server, first a device is authenticated by the authentication server with the help of this device specific certificate. Then the data is sent to the server periodically in the form of fixed sized data segments. Each data segment is signed using the private key of the device, the data along with the signature of the data segment is sent to the server. The server then verifies the signature of the data using the public key of the device. Before the authentication server can verify this device specific certificate it should have the public key of the Private Certificate Authority. So the root certificate of the Private Certificate Authority is installed in the authentication server. Now the authentication server will be able to verify the device specific certificate sent from the devices. If there is a mismatch between the MAC address of the device and the MAC address in the certificate the device will not be authenticated.

The whole implementation is divided into four parts.

- Generating the public and private key pair for the Private Certificate Authority and also self sign the certificate. This acts as the root certificate.
- Generate a sample public and private key pair for a particular device and generate a certificate signing request with the help of MAC address.
- The signing request is processed by the Private Certificate Authority and is signed by its private key.
- Push the root certificate of the Private Certificate Authority to the Authentication server trust store.

## Conclusion and Future Work

IoT is proliferating rapidly for all type of real time works. Providing secure communication between devices is challenging task since the devices are connected with internet. As providing 100% security is hypothetical right now we put our effort in maximizing the security for the devices. Our proposed security framework provides security by detecting and restricting the rogue devices in the network. We used MAC address with certificates for authenticating the devices. Our proposed framework enhanced the security with advantage of zero cost certificates.

Our future work will be to avoid alteration and maintain integrity by digitally signing the device firmware, make the device tamperproof using microcontroller chips and obfuscate the entire device firmware and the data by encrypting the firmware so as to make it difficult for an attacker.

## References

[1] K. Ashton. (2009, Jun.). Internet of things. RFID J. [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[2] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. Ad Hoc Networks. 2012; 10(7):1497-1516.

[3] Evans D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything [Internet]. Cisco IBSG, 2011 [cited 27 April 2015]. Available from: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] L. Xu, W. He, and S. Li, Internet of things in industries: A survey, Industrial Informatics. IEEE Trans. 2014; 10(4): 2233-2243.

[5] Zhou L, Chao H. Multimedia traffic security architecture for the internet of things. IEEE Network. 2011; 25(3):35-40.

[6] Chen D, Chang G, Jin L, Ren X, Li J, Li F, editors. A Novel Secure Architecture for the Internet of Things. Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on; 2011: IEEE.

[7] Fischer K, Gesner J, editors. Security architecture elements for IoT enabled automation networks. Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference on; 2012: IEEE.

[8] Li X, Xuan Z, Wen L, editors. Research on the architecture of trusted security system based on the Internet of things. Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on; 2011: IEEE.

[9] Abie H, Balasingham I, editors. Risk-based adaptive security for smart IoT in eHealth. Proceedings of the 7th International Conference on Body Area Networks; 2012: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[10] Jara AJ, Zamora MA, Skarmeta AF, editors. An architecture based on internet of things to support mobility and security in medical environments. Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE; 2010: IEEE.

[11] Yoshiaki Watanabe, Makoto Otani, Hirofumi Eto, Kenzi Watanabe and Shin-ichi Tadaki. A MAC address based authentication system applicable

to campus-scale network. Network Operations and Management Symposium (APNOMS), 2013 15th Asia-Pacific.

[12] Yun-kyung Lee, Jong-wook Han, Kyo-il Chung. Home Device Authentication Method in Ubiquitous Environment. Consumer Electronics, ISCE 2007. IEEE International Symposium.

[13] Soobok Shin, Hongjin Yeh, Kangseok Kim. An effective device and data origin authentication scheme in home networks. Emerging Technologies for a Smarter World (CEWIT), 2012 9th International Conference & Expo.