Security Challenges for Fog Computing enabled Internet of Things from Authentication perspective

Upendra Verma[a], *Dr. Diwakar Bhardwaj*[b]

[a]*Research Scholar, Dept. of Comp. Engg. & App., GLA University, Mathura , India*
[b]*Professor, Dept. of Comp. Engg. & App., GLA University, Mathura , India*

Abstract:

Fog-enabled IoT is a new paradigm that extends the Cloud computing platform by providing services and resources on the edge of network and also integrated with Internet of Things. Our paper proposed a Fog based Internet of Things platform where computing and storing services deployed on the edge of network to provide excellent services to users. For efficient IoT development, fog computing based IoT proposed which is the future IoT infrastructure. This paper first explores a comparison between Fog Computing and other technologies. Security issues are presented in Fog-enabled IoT system. Authentication plays important roles in realizing security issues. So this paper also investigates issues related to authentication and presented a security model for authentication between Intermediate storage (Fog Node) and Data centre (Cloud System). At the end of paper, AES is discussed which will be useful to implement our proposed system in resource constrained environment and finally discussed some open research issues and questions from the authentication point of view.

Keywords: Internet of Things, Fog Computing, Authentication, AES

I. Introduction

Internet has played vital role today. Everything around us connected to internet day by day with digital identity. With the development of Internet Technology, Internet of Things has become more important part of daily human life. Internet of Things are broader area as compared to Internet of computers. Now a day's things can be smart and digital. So all the things around us connected to internet to achieve high degree services for the useful life**.** There are many definitions of IoT proposed by many author. The most popular definition of IoT is "A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interface and are seamlessly integrated into the information network, often communicate data associated with users and their environments (Ian G Smith,2012) and the definition has been published and This definition of IoT to put some of the terms into perspective: Dynamic & Self-Adapting, Interoperable Communication Protocols, Unique Identity, Integrated into Information Network, Self Configuring.

The terminology "Internet of Things" was coined by Ashton K. in 1999 in MIT lab (Ammar Rayes, Samer Salam, 2017). The first IOT infrastructure "Internet connected coke machine" realized in 1982 and was installed in Carnegie Mellon University. It is estimated by various research communities that around 50 billion physical devices will be connected to the internet by 2020 (. Evans. D.,2011). IoT has three issues. First, Heterogeneity is discussed in the aspects of different sensing, processing and storing component. Traditionally only computers are connected to the Internet. Now heterogeneous things around us with digital identity are connected to Internet.

Second, Scalability is the key solution to handle explosive growth in the IoT ecosystem. When you deploy IoT system, it must be remember current and future need of the system. IoT system will not be able to accommodate future expansion due to lack of scalability. There are three keys to ensuring scalability in IoT—Develop of a system for ease of expansion, Demand device durability and Align network and device longevity.

Physical Things
Data and Services
Connectivity
Users with End Devices

Figure 1 Scenario of Scalability
(Different entities participating in IoT)

Third, Interoperability means number of heterogeneous devices are working together to achieve high degree of goal in IoT ecosystem. So it is the most essential need of IoT devices to interoperate with each other. For example a WiFi enabled laptop cannot be connected to Bluetooth enable mobile phone. This is the issue of interoperability. (Md. Iftekhar Hussain, 2016) suggested some possible approached to solve interoperability issues: Protocol Translation, IPV6 over WSN, Web of Things (WoT), Designing a generic Protocol Stack, Service Oriented Middle-ware (SOM). Most of the proprietary protocols (Z-Wave, Zigbee, Bluetooth Low Energy etc.) and IP based protocol (6LoWPAN, RPL etc) to solve the aforementioned issue.

Figure 2 Scenario of Interoperability

The full fledged security solutions cannot be implementing in IoT environment due to many security challenges. IoT architecture is not standardized. Most of researched utilized 3 tier or 5 tier architecture based on the requirements of IoT application and single architecture of IoT is not universally accepted. Fog computing is a new paradigm which supports Internet of Things to facilitate services to users and society. Fog computing has several characteristics compared to other technologies (cloud and edge) such as location awareness, low latency, capacity of processing high priority data, end devices mobility etc. Open Fog Consortium (OpenFog Consortium, 2018) was founded on Feb. 2017 and working toward to standardize architecture for fog computing.

This article is divided into following sections: Section II describes the Fog computing architecture from IoT system point of view. Comparisons of Fog Computing with other technologies are discussed in Section III. Section IV discussed security challenges in Fog-enabled IoT system. Section V addressed the issues of authentication in Fog Computing. Research Challenges in authentication is discussed in Section VI. Section VII concludes the article.

II. Fog Computing Architecture (Interaction Model) from IoT system point of view

Cicso was coined the terminology “Fog Computing” (Chiang, M., Ha, S., Chih-Lin, I., Risso, F. and Zhang, T., 2017). Fog computing is introduced to deal with the limitation of Cloud Computing. Fog Computing platform is introduced to support Internet of Things. Fog computing nodes can process high priority data that needs to be addressed immediately. The fog nodes are the closest to IoT devices and process high priority and delay sensitive data. The data generated by IoT device have lower priority can be directed to cloud server for further analysis and processing. The architecture of Fog computing is similar to Cloud computing. Fog computing supports virtualization (Chang, C., Srirama, S.N. and Buyya, R. , 2017). There is no existence of fog computing without cloud computing.

Fog based Internet of things divided into three layer: IoT Device, Fog layer and Cloud layer as shown in figure 3. Fog layer consists of various types of fog nodes such as smart phone, edge router, gateway, switches etc. EU's (end user) devices and IoT devices are the part of end user layer (Dang, T.D. and Hoang, D., 2017).

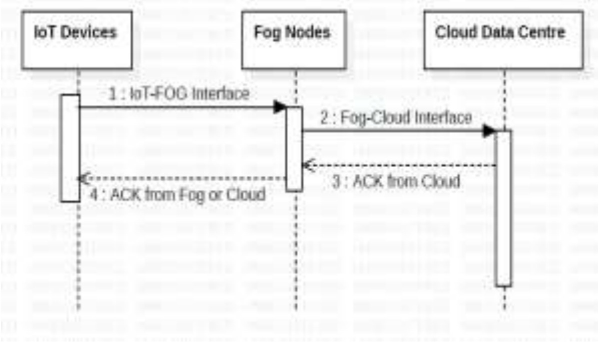

Figure 3 Fog enabled IoT model (Horizontal Architecture)

III. Comparison to other technologies

Cloud Computing v/s Fog Computing:

- Cloud Computing System have large computing and storage resources when compared to Fog Computing System
- In Fog Computing, fog nodes are distributed based on geographical locations when compared to Cloud System
- Fog computing supports M2M (Machine to Machine) communication
- Cloud System cannot be installed on low specification devices by Fog System can installed
- Fog system is located at edge of network compared to Cloud system
- Fog system can process high priority data immediately as compared to Cloud system
- In general, Fog System will operated locally

Edge Computing v/s Fog Computing:

In general, Edge computing and fog computing are interchangeably used because main aim of both computing are same. However, they can be differing with respect to how to process and handle data. In edge computing, each individual edge node is responsible to process data locally whereas fog computing, fog node is responsible to process data using its own resource or send to the cloud. Edge computing are not provided several services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These services can be provided with fog computing (Mithun Mukherjee, Lei Shu, Mohamed Amine Ferrag, Vikas Kumar, 2017).

IV. Security Challenges in Fog-enabled IoT Environment

Fog computing is integrated to Internet of Things and develop a new environment called Fog-enabled IoT Environment. If Fog computing integrated with IoT, then there are some challenges which should be addressed: First, how to manage fog computing infrastructure to allocate available resources to EU's or IoT devices. Fog Node has limited processing and storage capability. So, Fog nodes should be efficiently managed to provide services to IoT devices. Second, how to manage efficiently manage interface between IoT and fog nodes. The existing cryptographic techniques are not capable to process highly security feature on low power and resource constrained devices. There are complex security requirements to be deployed on Fog-enabled IoT platform. It is very challenging task to address security and privacy issues in Fog-enabled IoT system.

There are no standard certifications and measures of security defined for Fog-enabled IoT System or itself Fog Computing. Full security suite solutions would be difficult to execute in Fog-enabled IoT system due to smaller computing resources. If fog node compromised by attacker then its easy to acquire sensitive information from both IoT devices and Cloud System. So fog node can be compromised easily by attacker due to more accessible compared to Cloud system. On Fog Computing platform, only limited security solutions are proposed to detect and prevent from attacks.

V. Authentication Issues of Security in Fog Computing

Authentication is the essential requirements between Fog Computing platform and EU's devices. Insecure authentication has been identified as main security concern in Fog computing (Stojmenovic I, Wen S, Huang X, Luan H,2015). Fog Computing platform doesn't have rigorous authentication protocol as per their requirements and specification based on the current state of authentication. Authentications play an important role for IoT devices security. Crypto-graphical operations are required for authentication protocol and unfortunate, IoT devices don't have enough computation power and memory to execute such operations. One of the important solutions to fulfil the authentication protocol requirements in resource constrained environment that computation and storage (fog Node) will execute authentication protocol for the resource constrained IoT device and IoT device will outsource such type of operation from the fog node.

It is one of the challenging issues in Fog IoT. Generally, Symmetric key infrastructure and Public Key Infrastructure are used to provide confidentiality, Integrity, Authentication, Non repudiation, Access Control and Availability. Both infrastructures are different with respect to numbers of keys, encryption approach, decryption approach, round functions etc. In symmetric key encryption, only single key is used for encryption and decryption and other hand two keys are used (PU: Public key for encryption and PR: private key for decryption). But, PKI (Public Key Infrastructure) is not efficient and suitable for resource constrained environment. There are different reasons-according to (Ning P, Wang R and Du W, 2005) PKI is more expnsive and consumes more energy as compared to symmetric technique. (Goodman J and Chandrakasan P, 2001) has give reason that large computation and processing involved in case of public key. (RSA Security, 2004) has give reason that PKI uses two keys: Public and Private key. There is some mathematical computation involved to link between public and private key. Private Key is derived with the help of public key. So, it's difficult to protect public key from outside attackers. PKI is more expensive in terms of communication as compared to symmetric key technique (. Ganesan P, Venugopalan R, Peddabachagari P, Dean A,Mueller F and Sichitiu M, 2015). Symmetric authentication method is more suitable due to key management problem (Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer). Two primitives of symmetric based authentication: Block cipher and Stream cipher. Stream cipher is weaker than Block cipher due to various facts (Dasgupta A., 2005):

- Time-Memory tradeoffs attacks are stronger against stream cipher than block cipher.
- Algebric attacks are more effecting on stream cipher than block cipher.
- Block cipher is strongly protected from correlation attacks as compared to stream cipher.

Various academician and researchers studied and worked on developing security model for authentication at different levels. Our model is focused on providing secure authentication scheme between Fog (Intermediate storage) and cloud data centre. In the figure 4, provide authentication between Intermediate Storage (Fog) and Data Centre (Cloud). AES-SHA is applied for secure authentication. SHA is used to check encryption and decryption key with Hash Value.

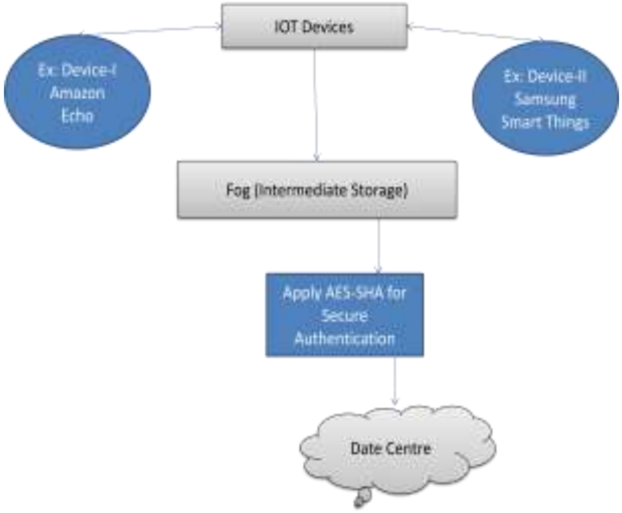
IOT Devices
Ex: Device-I Amazon Echo
Ex: Device-II Samsung Smart Things
Fog (Intermediate Storage)
Apply AES-SHA for Secure Authentication
Date Centre

Figure 4 Proposed Architecture for Secure Authentication

a) AES (Advance Encryption Standard):

AES is efficient encryption algorithm for fog computing and resource constrained environment. According to the study of multiple metrics such as user load against CPU time, utilization of memory, file size against encryption & decryption time, AES is university accepted (Mahajan P, Sachdeva A., 2013). AES was developed by NIST in 2001 as FIPS-197. It works on one of the primitives of symmetric key cipher: Block cipher. It operates on State (Block of data) and state has fixed size of 128 bits. Four rows and four columns are used to represent State. The defined key lengths are 128, 192 or 256 bits. Based on length of key, numbers of round functions are decided. 10, 12 and 14 round function iterations are operated based on the key length 128,192 and 256 bits respectively. Round function is used to transformed 128 bit state into modified 128 bit state.

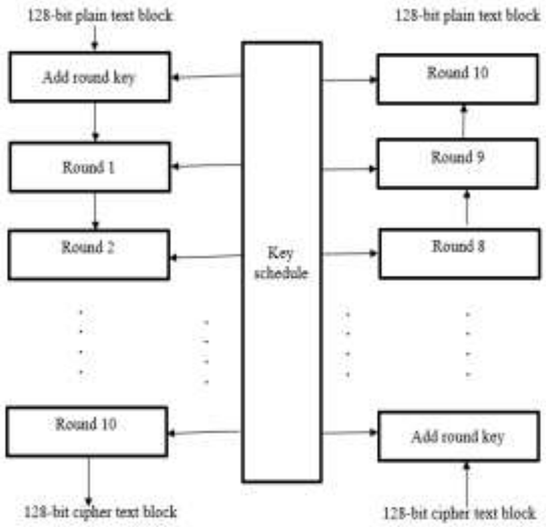

Figure 5 AES Block Diagram

a. SubBytes: Using 8 bit substitution box, each byte in the array (4*4 array) is updated in this step. S-Box performed Byte by Byte substitution of the block.

b. ShiftRows: It is a method of simple permutation.

c. MixColumns: Mix column transformation operates on each column individually. Each byte of a column is mapped into new value.

d. AddRoundKey: Round keys are generated by

Key Scheduling Algorithm. The first round key is equal to the private key/cipher key. Other round keys are computed.

AES is flexible for resource constrained environment and hardware implementation.

VI. Questions and Research Challenges from Authentication point of view in Fog Computing

Mobility of fog node is a critical issue in fog computing. The fog nodes join and leave a fog layer very frequently [10]. The major questions and research challenges from authentication point of views are as follow:

- When fog node joins or leaves the fog network then how to handle the security, privacy and authentication?.
- When fog node leaves the fog layer then how EUs can be preserved the privacy?
- How to design an authentication protocols between fog node and end users (EU's)?
- How Cloud Service Provider (CSP) detects user misbehavior in the presence of fog layer?
- How to trace the users by the cloud service provider?
- How to provide efficient and strong authentication mechanism with the help of symmetric key infrastructure?

VII. Conclusion

Authentication plays a vital role in Fog-enabled IoT system. In this paper, Authentication architecture has been presented between Fog and Cloud layer. Particularly, the differences between Fog, Cloud, Edge and three issues-interoperability, scalability and heterogeneity have been clarified at the outset. Security challenges from authentication point of view have been discussed. In addition, the paper also addresses the use of AES because of its computational and memory efficiency as compared to public key infrastructure.

References

Ian G Smith (2012). The Internet of Things 2012 New Horizons, IERC-Internet of Things European Research Cluster

Ammar Rayes, Samer Salam (2017). "Internet of Things From Hype to Reality", Springer Nature

Evans. D. (2011). The Internet of Things: How the next evolution of the internet is changing everything. Cisco white paper,1-11

Md. Iftekhar Hussain (2016). Internet of Things: Challenges and research opportunities, Special Issue ICAC 2016 of CSIT, DOI: 10.1007/s40012-016-0136-6, CSIT

OpenFog Consortium (2018) Accessed on: 30 July 2018 [Online]. Available: https://www.openfogconsortium.org

Chiang, M., Ha, S., Chih-Lin, I., Risso, F. and Zhang, T.(2017). Fog Computing and Networking: Part 1 [Guest editorial]. IEEE Communications Magazine, 55(4), pp.16-17

Chang, C., Srirama, S.N. and Buyya, R. (2017). Indie Fog: An Efficient Fog-Computing Infrastructure for the Internet of Things. Computer, 50(9), pp.92-98.

Dang, T.D. and Hoang, D., (May2017). A data protection model for fog computing. In Fog and Mobile Edge Computing (FMEC), Second International Conference on (pp. 32-38). IEEE

Mithun Mukherjee, Lei Shu, Mohamed Amine Ferrag, Vikas Kumar (2017). Security and Privacy in Fog Computing: Challenges, “IEEE Access”, DOI: 10.1109/ACCESS.2017.2749422

Stojmenovic I, Wen S, Huang X, Luan H (2015). An overview of fog computing and its security issues, Concurrency and Computation: Practice and Experience

Ning P, Wang R and Du W (2005). *An efficient scheme for authenticating public keys in sensor networks*, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL, USA, pp. 58-67

Goodman J and Chandrakasan P (2001), *An Energy Efficient Reconfigurable Public Key Cryptography Processo*”, IEEE journal of solid state circuits, pp. 1808-1820

RSA Security (2004), *Cryptography*, Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2152

Ganesan P, Venugopalan R, Peddabachagari P, Dean A,Mueller F and Sichitiu M (2003), *Analyzing and modeling encryption overhead for sensor network nodes*, In Proceeding of the Ist ACM international workshop on Wireless sensor networks and application, San Diego, California, USA

Strong Authentication for RFID Systems Using the AES Algorithm Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer

Dasgupta A.(2005), *Analysis of Different Types of Attacks onStream Ciphers and Evaluation and Security of StreamCiphers*, Available at:http://www.securitydocs.com/library/3235

Mahajan P, Sachdeva A. (2013) A study of encryption algorithms AES, DES and RSA for security, Global J. Computer Sci. Technol 13 (15):15-22