ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2018;3(1):27-30

RESEARCH ARTICLE

Security and Privacy in Fog Computing for the Internet of Things using Dynamic Digital Signature

B. Usharani

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Guntur, Andhra Pradesh, India

Received: 02-12-2017; Revised: 30-12-2017; Accepted: 09-02-2018

ABSTRACT

Internet of things (IoT) acts as technology integrator. IoT forms an intellectual environment by integrating the humans to the physical devices. IoT improves the availability and usability. IoT improves the resource utilization ratio. Fog provides data, compute, storage, and services to end users. Fog provides security in the cloud. Security to the fog of IoT devices is one of the greatest challenges in the world. This paper proposed a security technique for the fog of IoT devices. The proposed system uses a digital signature authentication technique to access the IoT devices.

Key words: Biometrics, cloud computing, fog computing, fog nodes, internet of things

INTRODUCTION

Internet of things (IoT) is the network of physical objects or things fixed with electronics. The technology of IoT has been improved according to the environment depending on the information communication technology and social infrastructure, combine IoT with the cloud. The benefit of this integration is the flexibility and the user gets in accessing the services that are presented by the cloud provider thought out the web interface. The term "fog computing" was introduced by the Cisco Systems, to simplify wireless data transfer to scattered devices in the IoT network. Similar to the cloud, fog provides data, compute, storage, and application services to end users. The objective of fogging is to progress efficiency and decrease the amount of data transported to the cloud for processing, analysis, and storage. This is frequently done to improve efficiency, though it may also be used for security and compliance causes. Fog computing applications include smart grid, smart city, smart buildings, vehicle networks, and software-defined networks [Figure 1].

Address for correspondence:
B. Usharani,
E-mail: ushareddy.vja@gmail.com

INTEGRATING FOG WITH IOT DEVICES [TABLE 1]

Thousands of things across the world are generating data; it is necessary to evaluate and operate on the data in less than a second. The fog nodes closest to the network consume the data from IoT devices. The fog extends the cloud to the closer to the things that produce and act on IoT data. These devices called fog nodes can be deployed anywhere with a network connection. Any device with computing, storage, and network connectivity can be a fog node. Examples consist of industrial controllers, switches, routers, embedded servers, and video surveillance cameras. Analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network, and it keeps sensitive data inside the network.
Fog nodes:

- Fog nodes observe or examine real-time data from network-connected things and then begin an action. The action can entail machine to machine communications or human-machine interaction.
- Receive data from IoT devices using any protocol.
- Run IoT-enabled applications for real-time control and analytics, with millisecond response time.
- Provide temporary storage, often 1–2 h.

Table 1: Comparison of various attributes to IoT devices in fog nodes to the cloud

Atrributes	Fog nodes closest to IoT devices	Fog aggregation nodes	Cloud
Response time	Milliseconds to subsecond	Seconds to minutes	Minutes, days, weeks
Application examples	M2M communication Haptics[2], including telemedicine and training	Visualization simple analytics	Big data analytics graphical dashboards
How long IoT data are stored	Transient	Short duration: perhaps hours, days, or weeks	Months or years
Geographic coverage	Very local: For example, one city block	Wider	Global

IoT: Internet of things

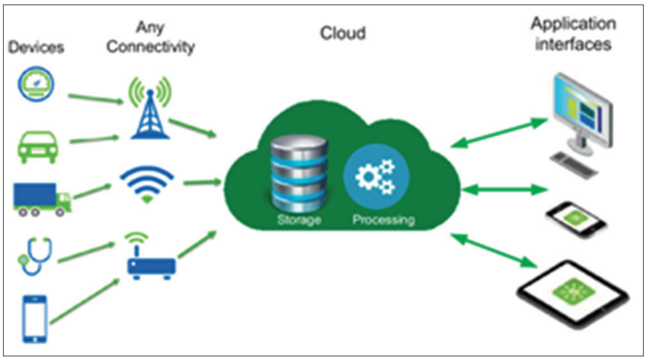

Figure 1: Connectivity between cloud and internet of things devices

- Send interrupted data summarizes to the cloud.

The cloud platform:

- Receives and combines data summarizes from many fog nodes.
- Perform analysis on the IoT data and data from other sources to gain business insight.

Can send new application rules to the fog nodes based on these insights.

BIOMETRICS

The term "biometrics" is derived from the Greek words "bio" and "metric." "bio" means life and "metric" means measure. Biometrics refers to technologies used to detect and recognize human physical characteristics. A biometric is a pattern recognition system including the hardware and software and their interconnecting infrastructure enabling identification by matching a sample to a stored pattern in a database. Biometrics is using to authenticate an individual using their distinguishable traits. There are two types of biometric methods [Figure 2].

1. Behavioral biometrics - used for verification purposes. This method looks at patterns of how certain activities are performed by an individual. Examples are keystroke or typing recognition, speaker identification or recognition, recognition based on typing speed, voice recognition, signature, gait, lip motion, AND dynamic signature.
2. Physical biometrics - used for identification or verification purposes. Examples are Fingerprint identification or recognition, speaker or voice authentication, hand or finger geometry recognition, retina recognition, face recognition, iris, DNA, ear shape, and odor.

The data can be represented either in one-dimensional (1D), two-dimensional (2D), or three-dimensional (3D) form. The biometrics using for 1D is voice and signature detection. The biometrics using for 2D is fingerprint, iris, hand, geometry etc. The biometrics using for 3D is face recognition.

SIGNATURE VERIFICATION [FIGURE 3]

Your body works as a password for smart devices:

- Static/off-line: The conventional way.
- Dynamic/on-line: Use electronically instrumented device.
- Principle: The movement of the pen during the signing process rather than the static image of the signature.
- Many aspects of the signature in motion can be studied, such as pen pressure, the sound the pen makes, etc.

Signature measures (dynamic)

- Speed.
- Velocity.
- Pressure.
- Static captured images.
- High user acceptance.

PROPOSED SYSTEM [FIGURES 4 AND 5]

Various technologies, such as smart grids, connected cars, and smart farms, have come forward based on IoT, and there is also the smart home, which is the fastest growing market. The smart home is that devices installed for various purposes connect to each other through the internet so that users can use the service anytime and anywhere. However, while the smart home provides convenience to users, recently the smart home has been exposed to various security threats, such as vulnerability of session/cookies and the use of vulnerable. This paper proposed a user authentication method using dynamic signature in the smart home and solved the problem of unauthorized smart home device registration of hackers by the application.

Privacy issues compact with hiding details, such as what appliance was used at what time. User data are encrypted and while permitting an accurate summary information data aggregation is carried out directly on cipher text at local gateways without decryption, and the aggregation result of the original data can be obtained at the operation center.

CONCLUSION

An overview of security and privacy issue is discussed in this paper. The aim of this paper is to solve different challenges in privacy and security in the fog computing of IoT. Security for the IoT is provided by the digital signature.The dynamic digital signatures are verified based on the speed, velocity, measures, shape of signature, and strokes. Privacy issues can acquire by encrypted the structured data and while permitting correct summary information. Data aggregation is presented directly on ciphertext at local gateways without decryption, and the aggregation result of the original data can acquire at the operation center.

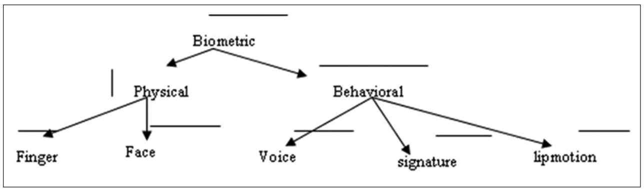

Figure 2: Biometric technique classification

Figure 3: Digital signature

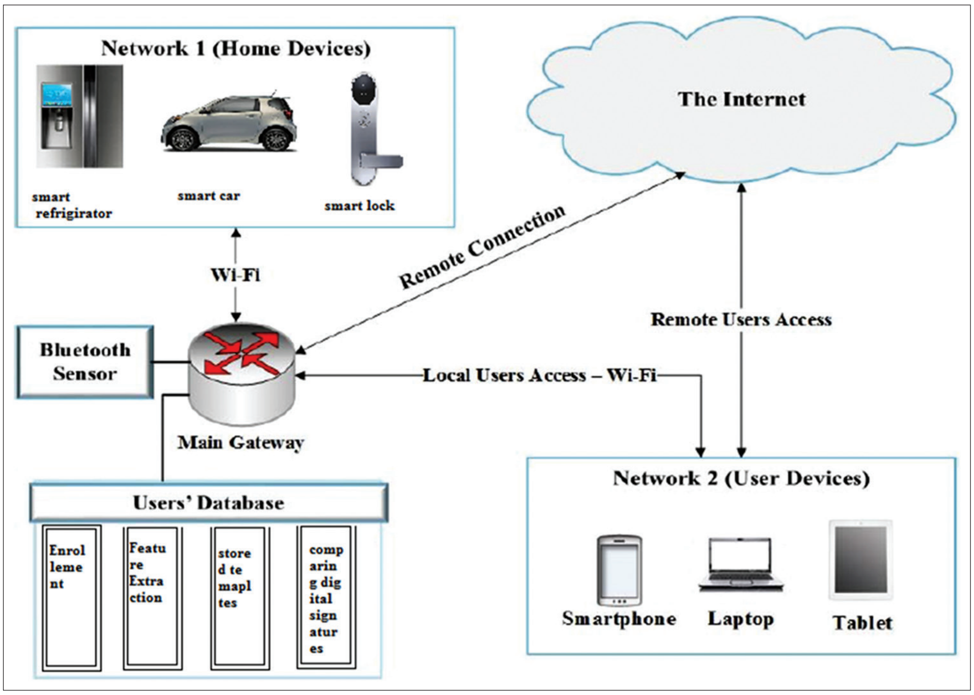

Figure 4: Proposed system

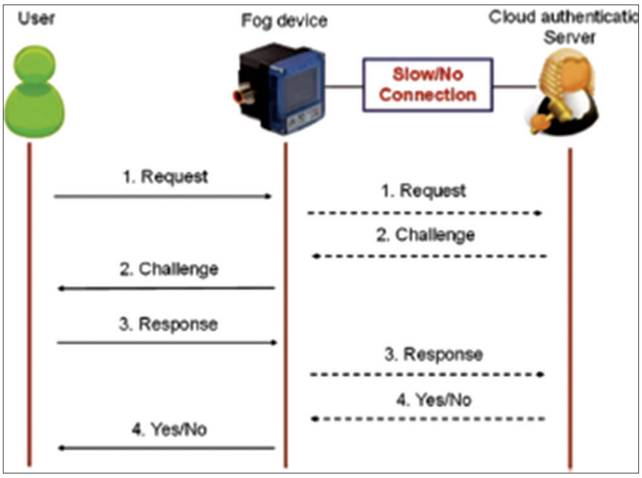

Figure 5: Authentication among the cloud and the fog

REFERENCES

1. IoT, From Cloud to Fog Computing. blogs@Cisco-Cisco Blogs.
2. Stojmenovic I, Wen S, Huang X, Luan H. An overview of fog computing and its security issues. concurrency and computation: Practice and experience. Concurr Comput 2016;28:2991-3005.
3. Bonomi F, Milito R, Zhu J, Addepalli S. Fog Computing and its Role in the Internet of Things, Workshop on Mobile Cloud Computing. ACM; 2012.
4. Bouzefrane S, Mostefa AF, Houacine F, Cagnon H. Cloudlets Authentication in NFC-Based Mobile Computing, Mobile Cloud IEEE; 2014.
5. Cash D, Jaeger J, Jarecki S, Jutla CS, Krawczyk H, Rosu MC, *et al*. Dynamic searchable encryption in very-large databases: Data structures and implementation. NDSS 2014;14:23-6.
6. Damiani E, di Vimercati DC, Paraboschi S, Samarati P, Violante F. A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks, CCS. ACM; 2002.
7. Dinh HT, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: Architecture, applications, and approaches. Wireless Commun Mobile Comput 2013;13:1587-611.
8. Intelligent Edge Intel. Available: https://www.itpeernetwork.intel.com/extending-intelligence-to-the-edge. [Last accessed on 2017 Feb 20].
9. Chiang M, Zhang T. Fog and IoT: An overview of research opportunities. IEEE Internet Things J 2016;3:1-11.
10. Bader A, Ghazzai H, Kadri A, Alouini MS. Front-end intelligencefor large-scale application-oriented Internet-of-Things. IEEE Access 2016;4:3257-72.
11. Varghese B, Wang N, Barbhuiya S, Kilpatrick P, Nikolopoulos DS. Challenges and Opportunities in Edge Computing. in Proc. IEEE Int Conf Smart Cloud (SmartCloud); 2016. p. 20-6.
12. Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: Vision and challenges. IEEE Internet Things J 2016;3:637-46.
13. Mahmud R, Buyya R. Fog computing: A taxonomy, survey and future directions; 2016.
14. Sarkar S, Chatterjee S, Misra S. Assessment of the Suitability of Fog Computing in the Context of Internet of Things. IEEE Trans Cloud Comput; 2015.
15. Yi S, Li C, Li Q. A Survey of Fog Computing: Concepts, Applications and Issues. In Proc. Workshop Mobile Big Data (Mobidata); 2015. p. 37-42.
16. Yi S, Qin Z, Li Q. Security and Privacy Issues of Fog Computing: A Survey. In Proc 10th Int. Conf Wireless Algorithms, Syst. Appl (WASA); 2015. p. 685-95.
17. Stojmenovic I, Wen S. The Fog Computing Paradigm: Scenarios and Security Issues. In Proc. Federated Conf. Comput. Sci. Inf.Syst. (FedCSIS); 2014. p. 1-8.
18. Stojmenovic I. Fog Computing: A Cloud to the Ground Support for Smart Things and Machine-to-Machine Networks. In Proc. Austral. Telecommun. Netw. Appl. Conf. (ATNAC); 2014. p. 117-22.
19. Kumar P, Zaidi N, Choudhury T. Fog Computing: Common Security Issues and Proposed Countermeasures. In Proc. Int. Conf. System Modeling Adv. Res. Trends (SMART); 2016. p. 311-5.
20. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Comput 2017;21:34-42.