ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 146

2nd International Conference on Artificial Intelligence: Technologies and Applications (ICAITA 2018)

Fog Computing and Security Infrastructure of Internet of Things

Xin Li* and Bo Yang

School of Information Management, Hunan University of Finance and Economics, Changsha, 410205, China

*Corresponding author

***Abstract*—Typically most data processing of IOT focuses on Cloud Computing. The huge amount of end devices and real-time data transmission leave great pressure on network bandwidth and Cloud Computing data centers. The paper suggests the introduction of Fog Computing between data centers and end devices of IOT to store and process massive local data on time, and to response most requests quickly and efficiently, thus to play an important role in security framework of IOT.**

Keywords—fog computing; cloud computing; internet of things; security infrastructure

I. INTRODUCTION

In 2005, Internet of Things (IOT) was officially named by the International Telecommunication Union (ITU). It has quickly become a development highlight of the Internet economy. By 2020, more than 50 billion end devices will be connected to the Internet of Things, and this figure will reach one trillion soon. These vast amounts of equipment include sensors, actuators and intelligent terminal, which produce large amount of real-time data every second. Traditionally, all data processing are dependent on cloud computing.

Cloud computing can supply and deploy a lot of computing resources dynamically, and provide service on-demand. This overcomes the deficiencies of traditional application system, such as inefficient utilization of system resources, limited physical space, complicated application deployment, and inflexible operation. However, with the characteristics of information distribution and exchange, cloud computing also faces great challenges.

- To support cloud computing, the network infrastructure requires the ultra-high speed switching, unified exchange, virtualization exchange, and transparent exchange, in which most existing network infrastructure hardly achieve.
- The information collected and exchanged in the Internet of things is vast, multi-source heterogeneous, redundant, complementary and real-time. The mass data needs rapid processing and transmission. Cloud computing is a highly aggregated computing service. It's simple and convenient to use, but it consumes too much network bandwidth. With the increase of user access, it is likely to cause some service interruption, response delay and so on.

The global research on the security of the Internet of Things had been found in various kinds of literature since 2011. The security infrastructure of the Internet of Things is faced with four major challenges: traceability and integrity of data, identification, trust management, and privacy protection. The focus of these studies is on data remote processing security. According to the characteristics of Internet of Things, light-weight encryption elements are proposed in embedded devices with limited resources to build a new security architecture of IOT [1].

Similar research in China started almost at the same time. Their main opinions argue that because of multiple heterogeneous of IOT, it is difficult to establish one unified set of security protection standards, but it should take different measures for different security problems faced by the three levels of IOT: perception layer, transport layer and application layer, and to construct a mixed networking security mechanisms [2].

For the great number of IOT end devices with limited resource, many Chinese researchers have proposed using lightweight security technology on perception layer of IOT to save resource consumption for storage, processing and transmission of information, and to improve response speed, and to avoid excessive pursuit of high-level security, and to provide appropriate security protection under the resource constrained situation [3].

On the IOT perception layer, many sensors and embedded devices can be implanted into relatively simple security measures, such as hardware based physical anti-copy function and light-weight encryption method. However, these security measures generally have the following shortcomings [4]:

- Because of the weak computing power and small storage capacity of the terminal equipment, the security operation takes more time and the response of the service request is slow.
- The energy supply of terminal equipment is limited, and the encryption method with high energy consumption is difficult to be completed normally.
- There are few data localizing, and the pressure of network bandwidth is great.

Therefore, these security means can only provide certain degree of security protection, and it is difficult to achieve a satisfactory overall effect. Starting from the most foundational Perception Layer to build the security system construction of

IOT, is conducive to the protection of all various parts of the system, but it must be considered how to devote more resources to the security system. Using fog computing in security infrastructure can utilize more local computing capacity and storage space, and meet the energy needs of all kinds of security measures which can be greatly enhanced. As result, all application request response time are significantly reduced, and network security system are also improved.

II. Analysis of Computing Advantages

In 2011, Dr. Flavio Bonomi, the president of global R&D Center in CISCO, and his researching team first proposed the concept of Fog Computing: The fog is between cloud computing and terminal computing; it is distributed service model with semi-virtualization architecture; terminal devices can access the local cloud network whenever and wherever possible (Local Cloud, also known as the fog node) [5, 6].

The fog computing layer includes both up and down gateways, and devices for temporary data storage and computing. It can judge different kinds of data requests. If these requests involve long-term data storage or historical data analysis, the layer will directly upload requests and data to cloud data center directly as gateway, otherwise data will be completely processed and stored locally. Fog computing not only inherits the advantages of cloud computing, but also has the advantage of edge computing. It can bring the advantage of terminal computing and local processing into full play. The nearest processing can effectively support rapid response for latency-sensitive applications, whose operations are often in the data center edge, such as traffic control system, parking system, health care system, local energy network system, etc.

With the introduction of Fog Computing, the resources that can participate in the edge computing will be significantly increased. Fog computing is a distributed computing service system. Its most outstanding operation characteristic is that the edge computing tasks can also be completed by gateway devices such as gateways, routers and access nodes. The current network equipment always has more powerful CPU and larger memory size, comparing to those earlier personal computers. Their location in the network can easily form a cluster, which can further integrate many edge nodes in distributed computation and storage capacity and form a more powerful fog node cluster. This cluster provides not only relatively sufficient computing power and data storage space, but also sufficient energy that the layer can use, avoiding the bottleneck for processing capability.

Fog calculation is not a substitute for cloud computing, but a powerful supplement. The fog computing layer can intelligently analyze whether the application requests need intervention from the cloud computing layer. For those real-time or low-delay requests, such as real-time data stream service, intelligent traffic monitoring, intelligent parking, etc., the system will call the fog computing equipment and local workstations and small storage units as quickly as possible to complete the response.

The fog computing layer can be regarded as a system composed of multiple independent fog nodes (Fog Node). Each node can contain several computing locations physically or logically, including the computing environment of application services, resource center, management and control center. The user interaction between nodes can be a remote Web communication mode or a local interaction. Users between nodes can access local and remote cloud service center resources. The changes in computing environment can cause synchronous migration of processing location and services, but the users' resource centers are always in a relatively stable [7].

III. Multi-layer Security Measures Based on Fog Computing

The Internet of Things can be logically divided into three main levels: the perception layer, the transmission layer and the processing layer. In addition, application data formed by the processing layer can also be regarded as an application layer. However, the basic security architecture of the Internet of Things must cover every logical layer, and the fog computing layer is mainly distributed closer to the perceptual layer. (See the Figure I)

For the hardware and the embedded device layer, under the fog computing layer, researchers have proposed to take different security measures and start from the bottom to meet the security challenges of the Internet of Things [8]. For example, sensor physical layer can use anti-clone functions (Sensor PUF, Physical Unclonable Function) to keep data security traceability and integrity; the sensors and other hardware PUF can be used to solve identification problems; PUF and hardware performance counters can strengthen the credibility management; lightweight encryption algorithms can support confidentiality and privacy protection [2].

There are many cryptographic elements that can be used for security protection of the Internet of Things, including encryption algorithms, HASH functions, digital signatures and key exchange algorithms. In order to consume less energy, it is essential to select appropriate processing sites and appropriate cryptographic algorithms based on the size of the data. For example, if the data to be processed is less than 1KB, sensor data processing is the best; if the data to be processed is less than 1MB, the data processing should be done in the fog node; if the data is less than 1GB, or more than 1GB, the data processing must be respectively in the joint infrastructure gateway or higher (including computing, storage and network communication ability). This fully localization of data processing brings faster response.

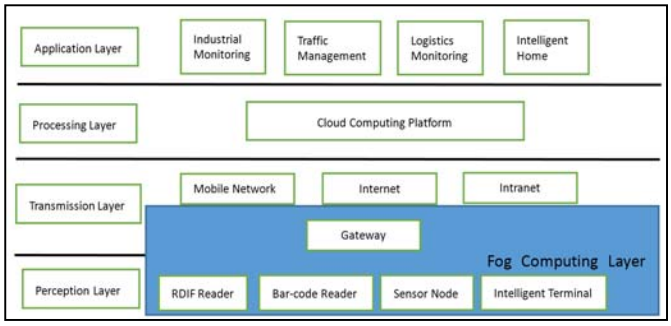

FIGURE I. FOG COMPUTING LAYER OF IOT

Various kinds of sensors in IOT have adopted more and more powerful single-chip microcontroller to build a complete single-chip system, such as ADc841/842/843 Flash Microcontroller, which already contains a 8052 kernel with the operation cycle of up to 20MHz, built-in 64KB flash and 4KB flash program data, 2304 bytes of data RAM, and a large number of peripherals, such as 12 ADC/DAC, a time interval counter, serial I/O, watchdog timer and power monitor etc.. This class of on-chip systems is enough to support lightweight encryption.

The sensor gateway of IOT is fully supported by power and hardware. The16/32 bit RISC processor and embedded Linux structure are often used. Its computing power is basically equivalent to a personal computer, and is fully capable of providing encryption protection with higher security performance.

International researchers have studied and summarized the encrypted elements available in the various layers of the Internet of Things, and made the following recommendations: [2]:

TABLE I. ENCRYPTED ELEMENTS IN VARIOUS LAYERS OF IOT

Items	**Deployment Layer**			
	Sensor	***Node***	***Gateway***	***Infrastructure***
Encryption Algorithm	**PRESENT mCRYPTON**	**CLEFIA AES**	**AES ECC**	**RSA**
HASH Function	**DM-PRESENT**	**PROP**	**HMAC**	**SHA-3**
Key Exchange Algorithm	**DH-512**	**DH-512**	**ECDH**	**DH**
Digital Signature	**ECDSA-163**	**ECDSA -233**	**DSA**	**ECDSA 409**

The construction of IOT security architecture based on fog computing layer will face three main problems: choosing the appropriate hardware configuration for Fog Computing, building and verifying appropriate encryption methods, and locating appropriate security measures deployment locations. The main work should focus on several aspects: to analysis time delay and power consumption of existing lightweight encryption algorithms used in the new fog layer, and improve the existing encryption algorithm or chose stronger security algorithm. The object should be a more consolidated security architecture of IOT based on fog computing with significantly reduce of time delay, same security, less power consumption, and optimized system response.

To build such security system of IOT, the key is to make full use of all kinds of resources distributed in fog computing layer, such as computing power, storage space and energy supply. To maximize the security strength of existing security measures, the key issues would include:

A. Optimization Strategy of Security Algorithm Based on the Sensor and other Hardware

Generally, the traditional sensor collects the objective value, produces the corresponding digital measurement results and encrypts and uploads. In order to improve the security strength, it can be tried to collect the uniqueness of sensor ID, and modify the corresponding security algorithm in the sensor. The uniqueness of ID is also used as the parameter of encryption algorithm, which affects the output result..

B. Improvement Strategy for Lightweight Security Algorithms

Subject to limited resources, the current terminal of the Internet of Things always uses lightweight security algorithms. With the introduction of sufficient computing power and memory space in fog computing, it is fully capable of supporting security algorithms with higher security strength and more complex calculation. On the basis of fully researching the existing lightweight security algorithms, it can be possible to improve security strength, speed up operation and maintain or reduce power consumption by properly algorithm improvement.

C. Evaluation Measures of Resource Supply on Fog Nodes

Fog computing layer is not a simple assembly of fog nodes, and multiple nodes can form a cluster to achieve efficient integration of resources. Based on some proper pressure testing, researcher can grasp the maximum resource potential that fog computing layer can provide, form a relatively stable node resource evaluation algorithm, and provide tools for future Internet of Things planning.

D. Evaluation Criterion on Improvement of the Security Algorithm

The improvement effect of the security algorithm can be measured by many indexes, such as the length of operation time, the size of power consumption and the strength of anti-attack ability. During continuous correcting and testing of the security algorithm, the quantitative calculation method of the above indexes can be achieved to form a set of objective evaluation criterion for the improvement of the algorithm.

IV. APPLICABLE EXPECTATION

The research of IOT security infrastructure based on fog computing has not only theoretical significance, but also broad application prospects and very important engineering value of system data traceability and integrity, credibility management, identity authentication, confidentiality and privacy protection and many other fields. The upgrading of the security system of IOT can win more user trust to Internet of Things system, and is of great significance for the development and popularization of the Internet of Things.

REFERENCES

[1] Cisco. The Internet of Things - How the Next Evolution of the Internet is Changing Everything, 2011, pp. 2-3.

[2] Arun Kanuparthi, Ramesh Karri, Sateesh Addepalli. Hardware and Embedded Security in the Context of Internet of Things. [C] Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles (CyCAR '13) ACM New York, NY, USA,2013, pp. 61-64.

[3] Chuankun Wu. Main Technology and Challenges of IOT Security [J] Journal of Cryptologic Research, China 2015,2(1), pp. 40-53.

[4] Gen Yang, Jian Xu.Characters and Technology of IOT Security [J].Journal of Nanjing University of Post and Telecommunication (Nature Science),China.2010, 30(4), pp. 20-29.

[5] F. Bonomi. Connected vehicles, the internet of things, and fog computing [C] The Eighth ACM International Workshop on Vehicular Internet Working（VANET 2011）. Las Vegas, USA : ACM, 2011: pp. 1-2.

[6] Bonomi F, Milito R, Zhu Jiang, et al. Fog Computing and Its Role in the Internet of Things [C]. Proceedings of the first edition of the MCC workshop on Mobile cloud computing. New York, USA : ACM, 2012, pp. 13-14.

[7] Clickloud Company. Fog Computing Introduction.[EB/OL].[2011-11-20]. http://www.tsgsites -hostmonster.com/fogcomputing/.

[8] K. Rosenfeld, E. Gavas, and R. Karri. Sensor physical unclonable functions. In Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on, IEEE, 2010, pp. 112–117.