Journal of Engineering and Applied Sciences 12 (12): 3130-3132, 2017
ISSN: 1816-949X

A Study on Diagnosing Security Vulnerability Issues of Big Data and Internet of Things under IT Convergence

Jimoon Chung, Sung Choi, Chang J. Kee, Eunjee Song, Songchul Moon, Junggil Kim and Sichun Noh
Department of Computer Science, Namseoul University, Cheonan, South Korea, Korea

Abstract: The Internet of Things (IoT) system shows the characteristics of a smart device by mounting various sensors and communication functions to the system. The data generated in the IoT environment is beyond the range of processing within given cost and time. In this study, security vulnerability occurring in the IoT and big data environments is diagnosed. A new security vulnerability may occur in each component in IoT, since a component is connected to security vulnerability. The property of data generated in both the IoT and Big data environments is related to that of big data, so security vulnerability issues in these environments are related those of big data. When these issues are diagnosed based on this relationship, a security measure may be effectively achieved. This study shows the importance of and necessity for security in this new ICT environment and the factors that can lead to security vulnerabilities.

Key words: Security vulnerability, security issues, internet of things, big data, IT convergence environment

INTRODUCTION

The internet of things is the network of sensor devices such as sensor electronics, electronic appliances and others embedded with electronics, software, sensors and network connectivity that enables these devices to collect and exchange data. The IoT network consists of sensors for sensing a particular situation or environment (sensor node), a processor for processing the collected information and a data transmitting and receiving device (sink node). In IoT, a seamless communication and information delivery is achieved from a physical component such as a sensor to user service, so security vulnerabilities specific to each individual component may exist. A new security vulnerability may occur in each component in IoT, since a component is connected to security vulnerability. Big data is difficult to manage and analyze by conventional methods, since its data format is diverse and unstructured and its distribution speed is fast. The reason for doing research on security issues of both IoT and big data is that it may be more effective in achieving security measures when the relationship from the attributes of data generated in IoT and to that in big data is diagnosed. This study derives and diagnoses security issues of both IoT and big data in the IT convergence environment.

The structure of IoT network: The components of IoT as shown in Fig. 1 are humans, things, the internet and distributed services. Uniquely identifiable tools and devices are the range of things. The range of things are uniquely identifiable tools and devices. The interlocking process of IoT is connected to sensing-networking-information processing-intelligent relationship-information exchange between things. In order to apply IoT in real life, generic technologies need to be syntagmatically implemented. Generic technologies can be divided into the sensor and network hardware technology such as controllers and communication chips, the middleware software technology for storing and analyzing the data received from things and the application software technology that interprets, expresses and processes data as meaningful results. The sensor network technology is the very basic technology that recognizes, extract data from things and transmits them to the internet. The role of human in IoT environment is to implement IoT and utilize the final information. Human doesn't need to be involved on the operational stage, since the operation of things is automated (Chang *et al*., 2002; Schnackenberg *et al*., 2005).

MATERIALS AND METHODS

Security association between IoT and big data

Data collection process: Things is a simple, an off-the-shelf and a programmable device. IoT means that every thing is connected to the Internet in IoT. Even animals, plants and locations are connected to the internet

Corresponding Author: Jimoon Chung, Department of Computer Science, Namseoul University, Cheonan, South Korea, Korea

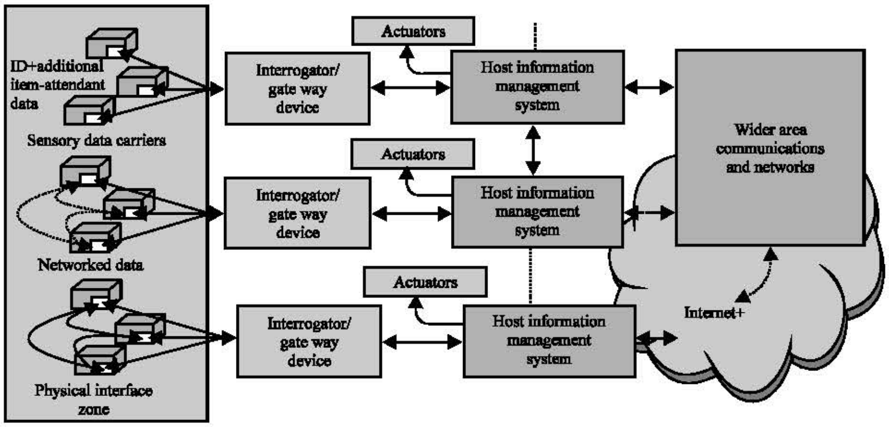
ID+additional item-attendant data
Sensory data carriers
Networked data
Physical interface zone
Interrogator/ gate way device
Interrogator/ gate way device
Interrogator/ gate way device
Actuators
Actuators
Actuators
Host information management system
Host information management system
Host information management system
Wider area communications and networks
Internet+

Fig. 1: The structure of IOT network: 2014 TATA consultancy services

as well as all kinds of goods and products. The concept of IoT is same with that of ubiquitous communications-anywhere and any object and assumes a connection to the internet. In IoT, an infrastructure is created where information between people and things and things and things is exchanged and communicated each other when all things of the world are connected, based on IT, via the Internet. Things are physical objects constituting the natural environment such as humans, vehicles, bridges, various electronic devices, eyeglasses, watches, clothing, cultural property, plants and animals. In IoT, the characteristics of smart devices by mounting various sensors and communications capabilities on things in the current application environment of IoT is shown. IoT generates the data beyond the range of data processing within given cost and time in a system, a service, an organization (or company). This feature as shown in Table 1, shows the generation process of big data in IoT environment (Schnackenberg *et al.*, 2000, 2001a, b).

Data attributes side: Big data as shown in Table 2, is structured or unstructured data that is too large, compared to existing data, to collect, store, retrieve, analyze and visualize by existing methods and tools. It is also data beyond the range of data processing within given cost and time in a system, a service and an organization. Even though big data has useful advantages as well as dangerous drawbacks, it will be actively used in marketing. It is information that has comprehensive consumer information such as gender, ages, hobbies, interests. Analyzing big data does not simply mean analyzing a large amount of data. System or service itself should have ability of adapting to big data as well as analyzing ability. Organization that plans, develops and operates systems or services should have ability to deal with big data. Big data can't be solved with one solution and should be solved with a variety of solutions, depending on the requirements and properties of data (ITU, 2016).

Table 1: Characteristics of data generated in IoT

Divisions	Characteristics
Data collection process	Data collected by the program by hand not machine
Property of data	Data-much finer than existing data, generated from machinery, sensors, programs such as click stream, meter
Data owners	Data from outside organization where the production and management of data is not possible
Data type case	Unstructured data - user data, such as video stream, image, audio, social networks, sensor data, application program data

Table 2: The property of big data source: NIA, securing data resources and quality control measures in the big data era, 2012

Variables	Data produced from computer	Data produced by human	Relationship data
Producer	Application server log (website, games, etc.); sensor data (weather, water, smart grids, etc) Image, video (traffic, security camera etc.)	Twitter, blogs, email, photos, bulletin board posts, etc.	Facebook, LinkedIn, etc.
Type	Orthopedic Structured data stored in DB	Half-orthopedic Web document, metadata, sensor data, process control data, call detail data, etc.	Atypical Social data, documents, audio, video, images, etc.

RESULTS AND DISCUSSION

Security vulnerabilities in the IoT and big data environments units

Security vulnerabilities at terminal aspects: The IoT terminals holds the vulnerabilities of its own. These are also same with the typical properties of information processing devices-hacker's attacks and malware infections. It can be seen that the attack patterns and threats threatening information security environment of

Table 3: The attributes of big data security quality

Divisions	Attributes
Confidentiality	Only the big data owner or a person who is authorized from the owner and a person who receive authorization from the relevant legal regulations can access to information
Integrity	Ensuring that the creation, modification and deletion of big data information by an unauthorized party is prevented
Availability	The user is given permission to use big data information services at any time
Certification	Accessing to inside big data information assets from outside, it should be authenticated
Repudiation	Prevent to deny the action of the information systems usage

IoT is equivalent to that of PC. Hackers tends to select attack targets that can generate a large amount of damage effect within a short time. Targets used to be devices which are popular and used extensively. Hackers attack or distribute malicious codes by utilizing OS vulnerabilities and protocol vulnerabilities discovered in Smart TVs. IoT devices are small computers and of course use OS. By using IoT devices, hackers may do search, use social networks and install new apps. Like security threats in the traditional database, data security threats in the IoT are serious threats. These can be threatening of spilling the backup of the entire file system with root privileges, spilling from insiders and exporting the data by using DB administrator's privileges.

Security vulnerabilities at data aspects: IoT may increase the analytical data, since traffic is increased and security threats are occurred by changes in various smart devices and the Internet environments. Data volume of IoT environment is based on size of the data. MIME data such as mail data or web log data is correspondent to several PB however, Twitter network data is less than several tens of GB. The analysis and processing of data is a significant concern. There is a difficulty in handling the attributes of data as shown in Table 3, since the properties of data, not the size of data, is important. The velocity means the speed of data processing. It is a function that returns the result of processing after processing a number of user requests in real time, if necessary. The various data is analyzed in the traditional enterprise data and stored in ERP, SCM, MES, CRM, etc. It is the operating data generated from within the enterprise.

CONCLUSION

In order to cope with security vulnerability in IoT and big data environments, it is important to encrypt and authenticate messages sent between the nodes for establishing a secure wireless sensor network environment. An encryption algorithm and the key management protocol are necessary for encryption. The protection of privacy is also necessary in large data processing created at the same time on different channels. In order to meet the constraints and requirements of the security sensor network, a technique including a light-weight and password authentication technology suitable for environmental sensors, light key management techniques, the privacy protection technology preventing side-channel attack and techniques must be used. The lightweight intrusion detection mechanism functions need to be applied to secure detecting node connected to the network. It is necessary to grasp the identification number of the terminal authentication techniques and systems for sensors unmanaged by humans. The increased traffic and security threats caused by changes in various smart devices and internet environments, quality control programs procedures need to be institutionally and procedurally organized.

ACKNOWLEDGEMENT

"Funding for this study was provided by Namseoul University".

REFERENCES

ITU., 2016. Internet of things global standards initiative. Technology University, Lahore, Pakistan. http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

Schnackenber, D., R. Travis, D. Kelly and W. Brett, 2005. Cooperative intrusion traceback and response architecture (CITRA). Master Thesis, Space and Naval Warfare Systems, San Diego, California, USA.

Schnackenberg, D., H. Holliday, R. Smith, K. Djahandari and D. Sterne, 2001a. Active Networks Intrusion Detection and Response (AN-IDR). Proceedings of the DARPA Conference on Information Survivability Conference and Exposition (DISCEXII'01), July 20, 2001, IEEE, Honolulu, Hawaii, pp: 1-13.

Schnackenberg, D., K. Djahandari and D. Sterne, 2000. Infrastructure for intrusion detection and response. Proceedings of the International Conference on DARPA Information Survivability Conference and Exposition Vol. 2, January 25-27, 2000, IEEE, Hilton Head, South Carolina, USA., ISBN:0-7695-0490-6, pp: 3-11.

Schnackengerg, D., H. Holliday, R. Smith, K. Djahandari and D. Sterne, 2001b. Cooperative Intrusion Traceback and Response Architecture (CITRA). Proceedings of the DISCEX'01 Conference on DARPA Information Survivability Conference and Exposition II Vol. 1, June 12-14, 2001, IEEE, Anaheim, California, USA., ISBN:0-7695-1212-7, pp: 56-68.