Journal of Engineering and Applied Sciences 12 (Special Issue 7): 8062-8065, 2017
ISSN: 1816-949X
© Medwell Journals, 2017

IoT and Wireless Terminal Security Technique

Wonseok Kim, Eunsik Bak and Euiin Choi
Department of Computer Engineering, Hannam University, Daejeon, Republic of Korea

Abstract: Recently, with the increase of IoT distribution, internet systems between wireless terminals and IoT are attracting attention. These IoT are communicated by digital transmission in the open space. IoT communicates each other via. the internet from anywhere in public. IoT in public space is exposed to a number of security threats. When user's information is exchanged through the IoT and the wireless internet between mobile devices, there is a possibility that the information could be leaked from. If the user information is leaked, the user will no longer be able to trust the IoT device. We propose an internet security system for IoT that can solve these security threats and send/receive information securely. IoT includes wireless internet, Bluetooth and so on. We suggest how to improve the existing problems of the internet.

Key words: IoT, wireless terminal, wireless communication, IoT security technology, internet, Bluetooth

INTRODUCTION

Recently, the market of IoT has been increasing and the business related to IoT is also increasing. Send and receive a lot of information from the public place to the digital transmission using these IoT equipment. It can be used in various fields such as remote control system while exchanging information between digital devices. This internet of IoT objects can be used in public places and security issues of the IoT also occur. Personal information may be leaked from the internet and the internet during the user's IoT and the wireless terminal and solutions to solve these problems should be provided. In this study, we propose wireless communication security improvements for solving the problem of existing IoT wireless communication security system.

Literature review

IoT: The concept of the IoT is defined variously in academia and industry. ITU is ITU-T World Summit on the Information Society's "ITU Internet Reports" The concept of the IoT was first presented. If the existing information and communication technology has enabled people and objects to exchange information anytime and anywhere, IoT adds a new concept of what is as shows in Fig. 1, to concept people, objects, people, objects. It is defined as a technology that enables communication. Here, "Anything" includes not only specific objects in physical space but also information that is identified and stored in virtual space. Cisco, a global telecommunications company in the United States, estimated the value of enterprises in IoT over the next decade to be $14.4 trillion. The number of devices connected to the internet in 2015 is estimated at 4.9 billion units which will increase to 25 billion units by 2020. The domestic IoT market is also increasing recently. Recently, many devices using IoT have been released. IoT is used in public as well (Kim *et al*., 2013).

Wireless terminal: In the IoT environment, the terminal attaches to a specific object, extracts data from the object and transmits the data to the other terminal or a gateway that manages the extracted data through the network. RFID, sensor nodes, smart devices, etc. and the gateway can process data transmitted and received using various heterogeneous network (Kwon *et al*., 2015).

MATERIALS AND METHODS

IoT security technique: Wireless communication security technology uses device behavior and devices to maintain security and support technology. In the IoT era, not only computers and smartphones but also tens of billions of different types of objects are connected to the internet. These IoT devices are often small devices with limited battery capacity and low computing power. Therefore, after data is generated without a separate encryption process, it is transmitted to the internet through other peripheral. If data are illegally collected or tampered with by a malicious user in this process, it could cause serious security incidents as well as violate personal privacy. Because IoT service connects the virtual world with the real world, hacking in cyberspace can be transferred to the risk of physical space as it is. IoT security threats can occur in the device, network and service areas that are components of IoT. IoT security threats include

Corresponding Author: Euiin Choi, Department of Computer Engineering, Hannam University, Daejeon, Republic of Korea

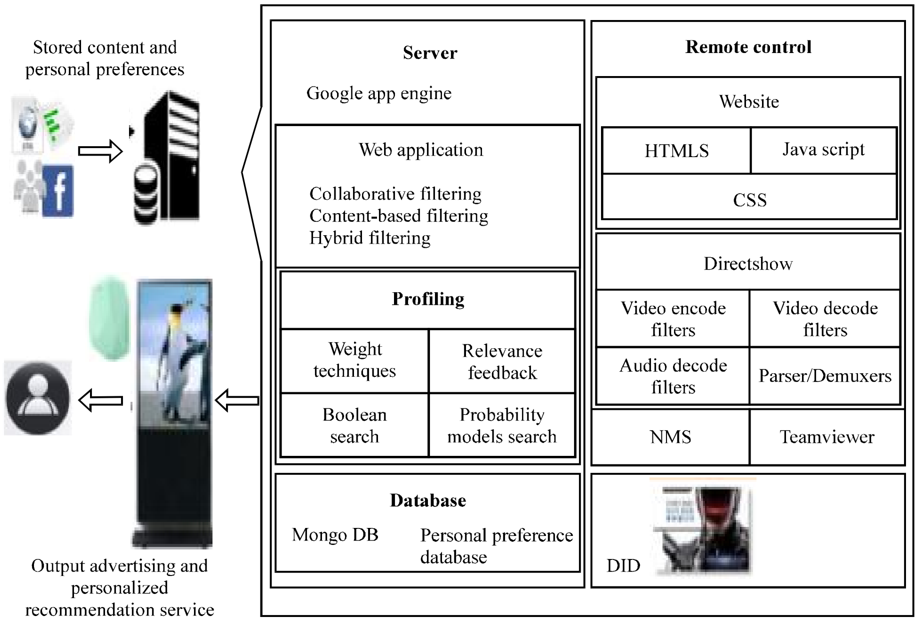


Fig. 1: IoT frame work (Be and Kim, 2015)

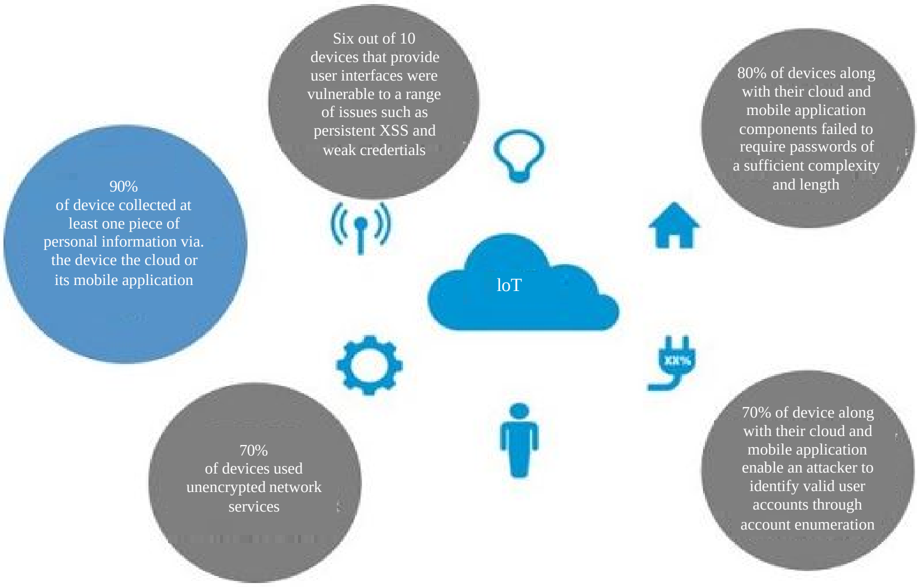

Six out of 10 devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credertials
80% of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length
90% of device collected at least one piece of personal information via. the device the cloud or its mobile application
IoT
70% of devices used unencrypted network services
70% of device along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration

Fig. 2: IoT security issues

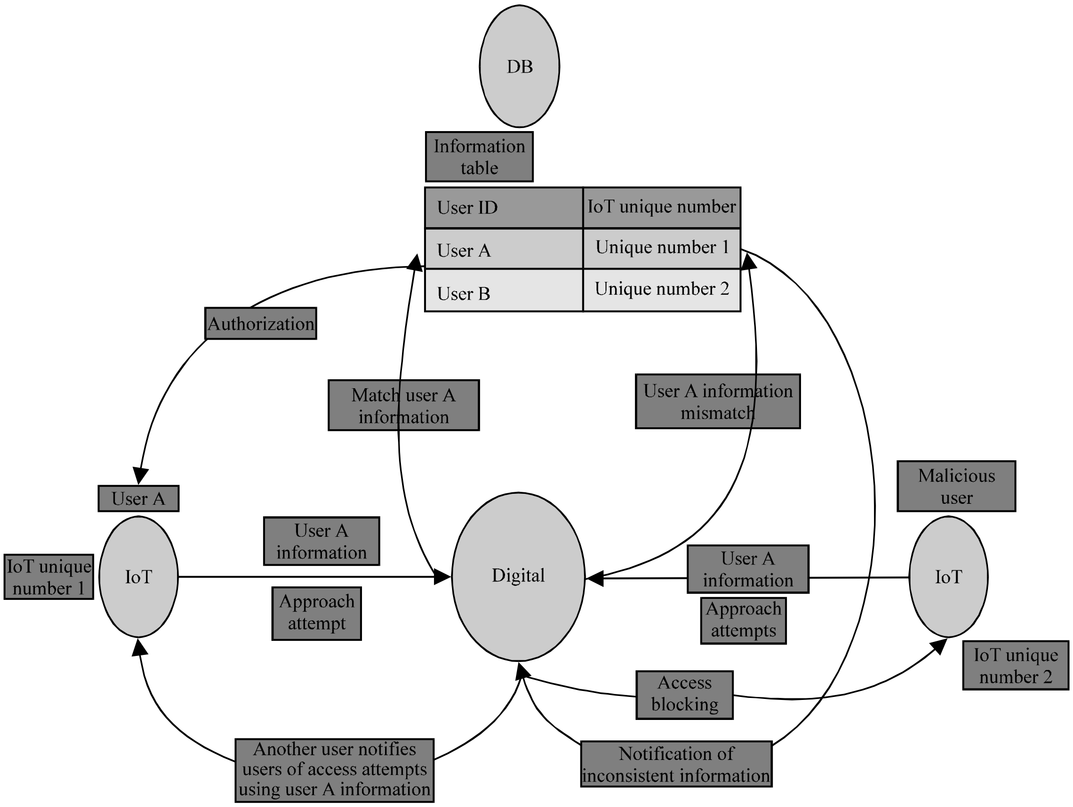
unauthorized access, replication attacks, information leakage, data forgery, denial of service, privacy breach. Unauthorized access refers to a security threat that an unauthorized attacker attempts to gain unauthorized access to a particular device, resource or service, manipulate it or physically damages. In addition, unauthorized access may cause information related to devices or users to be leaked which may immediately lead to privacy breaches. It may also degrade the quality of the IoT service by modifying the data generated by the device or processed by the system. Since, most IoT devices use wireless communication technology, it is also possible to embed the device by eavesdropping or sniffing the data that the smart devices transmit. You can prevent duplicate devices from sending services by sending spam or generating large amounts of data (Jang and Kim, 2014; Kim, 2014; KINEWS, 2014; Be and Kim, 2015) (Fig. 2).

Wireless communication security problem between existing IoT and wireless terminal: Among existing IoT security methods, the existing problem of authentication/authorization scheme is that a third party can use the information of the user to access the spoofing if the user's information is known at authentication/authorization . This problem is that once a user's information is exposed, all information can be leaked and existing methods are easy to leak. Typically, if IoT devices are used externally they can be visually exposed when they are authenticated by authentication/authorization technology these visual exposures need to be improved to avoid security problems (Lee *et al*., 2014; Kim and Jo, 2015; Kim, 2016; Lee, 2015).

RESULTS AND DISCUSSION

Proposed technique: Existing IoT products are difficult to improve security issues with authentication/authorization technology alone. Authentication/Authorization techniques can cause spoofing issues in addition to visual exposure this is a security issue that has been a problem in the past, ongoing research is underway to find improvements. To improve the problem, the following suggestions are suggested.

If the user authenticates through authentication/authorization with the user's IoT, even if the third party authenticates using the user's authentication information, access to the existing IoT is prevented, so that, access can't be made if the user is connected. In addition, the IoT unique identification number is specified and the IoT unique identification number is registered in the user authentication information, so that, the IoT unique identification number that does not match the IoT unique identification number registered in the user authentication information can't be authenticated/authorized. If a user attempts to log in with an IoT other than the IoT they have, they can track the malicious user attempting to log in with their IoT number. IoT GPS systems also require security points to track malicious users. Using this technology, the user's information is protected but the malicious user can also be traced which makes security highly efficient (Fig. 3).



User ID	IoT unique number
User A	Unique number 1
User B	Unique number 2

Fig. 3: Proposed model

CONCLUSION

As the recent spread of IoT increases, the necessity of related security technology is increasing. Kwon *et al.* (2015) security technologies are being developed to protect user information and related research is also underway. Therefore, this study presents the following solutions.

A system for matching and authenticating authentication/authorization information with a unique identification number possessed only by the user's IoT is. It can't be authenticated only by the user's authentication information and user's IoT unique identification number and authentication information must be matched, so that, they can be accessed. This technology solves the problems of existing authentication/security technology and can be applied to other fields. In addition to IoT, it can be applied to other wireless devices and it can be used as a security device because it can track malicious users. To use this technology, an additional system is required to match the user's IoT number and user information. Also, it is necessary to design an IoT GPS system to fundamentally track malicious users, it is necessary to develop a system that matches IoT unique identification number with user information. The IoT unique identification number and the contents of the user's information matching system need to be discussed and designed in the future.

ACKNOWLEDGEMENT

This research was supported by 2017 Hannam University Research Fund.

REFERENCES

Be, S. and J. Kim, 2015. Development of Internet of Things (IoT) and change in security paradigm. KISTEP. IntI., 14: 44-57.

Jang, B. and C. Kim, 2014. Research on internet of things security technology. Secur. Eng. Res. J., 11: 429-438.

KINEWS., 2014. Existing IoT products 80%, maintain security vulnerability. KINEWS Company, Mushin, Lagos, Nigeria.

Kim, D., S. Yun and Y. Lee, 2013. Security for IoT service. J. Inst. Telecommun. Eng. Korea Inf. Commun., 30: 53-59.

Kim, H., 2014. Security and privacy problem in internet of things environment. TTA. J., 153: 35-39.

Kim, S. and D. Jo, 2015. IoT (Internet of Tings) security technology trends. Korea Contents Soc. J., 13: 31-35.

Kim, S.H., 2016. Internet of Things (IoT) technology. J. Electron. Donating Soc., 43: 64-71.

Kwon, H., B. Chun and J. Kim, 2015. Current status of next generation IoT network security. Inf. Process. Soc. J., 22: 35-46.

Lee, H., C. Bak and S. Kim, 2014. Work effected with the same characteristics of IoT device. Inf. Sci. J. Software Appl., 41: 545-556.

Lee, S., 2015. Protection trend of information from Internet of Things (IoT). J. Korea Inst. Inf. Commun., 16: 28-35.