Increase Security of IoT Devices Using Multiple One Time Password

Niskarto Zendrato¹, M Zarlis¹, Syahril Efendi¹, E S Barus¹², Sulindawaty¹ Hasanul Fahmi¹

¹ Faculty of computer science and information technology, Universitas Sumatera Utara, Medan - Indonesia
²STMIK Kristen Neumann Indonesia, Jalan Jamin Ginting Km 10.5, Medan - Indonesia

*niskarto@usu.ac.id

Abstract. Lately more IoT use of devices both used at home, disaster prone, hospitals, highways and government agencies and many other places that use IoT device for data acquisition in realtime therefore the authors want to examine the security of IoT devices that is increasingly being used by utilizing OTP codes sent by smartphone devices or GSM modules to keep IOT devices from people who want to exploit the IoT device.

1. Introduction

In the era of information technology development is now widely applied IOT everyday life such as used as an earthquake sensor, light sensor and others. Age of the Internet of Things is already present. The impact of that era makes the activity more easily because everything is connected, such as a smartphone, smartwatch, television, vending machines in coffee shop, even including a thermostat which is already connected to the internet and can control the temperature in the house. With the principle of the main objectives of the IOT as a tool that makes it easy for the supervision and control of physical goods then the concept of IOT is very possible to use almost all daily activities, ranging from individual use, offices, hospitals, tourism, industry, transport, conservers animals, agriculture and livestock, to the government.

Within these objectives, the IOT has an important role in controlling electricity consumption, so that power consumption can be more efficient as needed from the level of personal consumption to the industry. Of course, in addition to saving purposes IOT also be used as a means of business progress, with the monitoring system can be more scalable business needs. IOT also very useful in the automation of entire devices connected to the Internet where the automation configuration can be adjusted easily without having to come to the location of the device. Good for safety reasons to areas that are not likely to enter a human, or for reasons that would reach to the device in the control.

Gartner, which is one of the well-known in technology research firm, estimates that in 2016 there are around 6.4 billion connected objects. And it is predicted that in 2020, the acquisition of these connected objects reach up to 20.8 billion. However, some existing IOT device is considered to have a very weak security system. Therefore, some of these devices has now become a soft target for cyber criminals, just like robbers who prefer to target homes without alarm or guard dogs. Last year, Symantec is a security system solutions provider to obtain report an increase in attacks so-called proof-of concept. The attack was allegedly aimed at IOT devices are quite dangerous. In many cases,
IOT devices are often weak in the implementation of action experience, and some can attack exploits a vulnerability in the Linux-based operating system that is found in some IOT devices and routers. So how should companies provide security for device IOT? Peter Sparkes, Senior Director of Cyber Security Services APAC and APJ, Symantec described some of the solution. The first step is always to protect the information while using smart devices, such as data to be encrypted, regularly change their passwords and usernames on a regular basis, do not be hasty in giving sensitive data. And when considering IOT devices, employees should use a layered approach to security, while ensuring comprehensive protection for their data through backups,

The use of one-time password (OTP) is quite common nowadays. OTP is a password that can only be used for a single session or a transaction. The method used to generate the OTP may include algorithms using a password that was raised earlier, or by using time. When using time passwords generated can only be used for a limited period only. Typically, the OTP is used as a method of user authentication via HTTP, using Authorization header. With this method, users need to enter a username and OTP resurrected. OTP is often used to avoid this type of attack when a transaction is repeated over and over with a valid unfavorable destination. Therefore, the authors want to analyze the application of the OTP for securing the device IOT to protect the device and the data contained on the device IOT, which is where the device IOT needs to be protected because IOT devices can be exploited by hackers as botnets and data on the device IOT can be manipulated by hackers so IOT devices may not work properly.

Formulation of the problem. The formulation of the problem in this research is how to implement the OTP on the device so that the safety of the device IOT for the better.

**Scope Of The Problem**

The thresholds problem in this study is the observation of several devices IOT and receiver using a smartphone as OTP code to the device is not directly. The Aim of this research is To study the security system IOT Improve the safety of the device IOT and IOT test device security level. The Benefit of this research As a source of reference for future research, As the device security platform IOT

2. **Literature Review**

2.1. **Security on IOT**

One of the challenges that must be overcome to encourage widespread implementation of IOT is the security factor. IOT is a pluralistic system. Its diversity not only because of the involvement of various entities such as data, machines, RFID, sensors and others, but also because it involves a wide range of devices with communication capabilities and data processing. The number of entities and data involved, making IOT face security risks that can threaten and harm consumers. This threat is mainly done by allowing an unauthorized person to access the data and misuse of personal information, facilitating attacks against other systems, as well as threaten the personal safety of its users. The threats that may affect the entity IOT vary considerably depending on the target of the attack.

a. Denial of Service, attacks that because legitimate parties cannot invoke the service.

b. Physically damaging objects in the IOT.

c. eavesdropping; passive attacks that can be performed on a variety of communication channels with the aim of extracting data from the information flow.

d. Node capture; attacker to extract information from the node or from any other infrastructure that has the data storage capabilities.

e. controlling; where the attacker tries to gain control over the entity IOT and disrupt service or data from the entity. Various types of threats in the above, it can attack the various entities in the IOT, especially RFID and sensor networks.

2.2. **One-time password (OTP)**

One-time password (OTP) is designed to address a replay attack. With OTP, the user identity that is sent through a computer network will be constantly changing, and only be used one time only. Thus,
although the attacker can steal user identities, the attacker will not be able to use a stolen identity. Systems that utilize One-time password must have a generator that can generate passwords based on user input. In addition, the server must be able to validate the password received. The server also must be able to provide participating seed used to generate the password.

OTP generation can be done in various ways, but the most common is to do a hash on the user's identity and the seed of the server. One method that utilizes the hash function is the method proposed by Leslie Lamport. This method works by performing a hash on the user's identity and the seed of n iterations to generate a password. Then, when the password is used, the password is stored on the server, then the number of iterations minus 1.

Next, when the user wants to perform authentication again, the number of iterations performed hash is n-1. To perform the verification servers simply compute a hash of the password, and compare it to the value already stored.

2.3. Smartphone

Smartphone is a smart phone that has the ability as a computer. Smartphones are classified as high-end mobile phone equipped with a mobile computing capabilities. With the capabilities of the mobile computing, smartphones have capabilities that cannot be compared with ordinary mobile phones. Smartphones, which first appeared a combination of functions of a personal digital assistant (PDA) with a mobile phone or a phone with a camera. Along with its development, now the smartphone also has a function as a portable media player, the low-end digital compact cameras, pocket video cameras and GPS. Modern smartphone is also equipped with a high-resolution touchscreen display, a browser capable of displaying full web like on a PC, as well as data access WIFI and broadband internet.

2.4. Cryptography

Cryptography is derived from the Greek, crypto and Graphia. Crypto means confidential and Graphia means writing. According to the terminology, cryptography is the science and art to maintain the security of the message when the message is sent from one place to another. Techniques for data encryption (cryptography) is applied to the data and information, carried out by encode or hide the original data. In cryptography, a message will be withheld called plaintext and encrypted messages that have been called ciphertext. The development of computers and communication systems in the 60's impact on demand of certain the others as a means to protect information in digital form and to provide security services.

2.5. Internet of Things (IOT)

Internet of Things (IOT) was first introduced by Kevin Ashton in 1999. Although it has been introduced since 15 years ago, until now there is a global consensus on the definition of IOT. However, the general concept of IOT is defined as an ability to objects connect smart and allows it to interact with other objects, the environment and with other intelligent computing equipment through the Internet. IOT in its various forms has begun to be applied to many aspects of human life. CISCO even have targeted that by 2020, 50 billion objects will be connected to the internet. Widespread adoption of IOT technologies, making human life becomes much more comfortable. In terms of individual users, IOT strongly influences the domestic field as in the application of intelligent home and car. From the user side of the business, the IOT is very influential in increasing production quantity and quality of production, overseeing the distribution of goods, prevent counterfeiting, shorten the time unavailable goods on the retail market, supply chain management, etc. IOT is used in a case of medical equipment applications connected monitor glucose in diabetic patients, will allow doctors to receive patient data in real time, monitor the patient's condition and adjust the dosage of medication.

Thus the disease management becomes easier to do. Similarly, the smart home application, that enables users to manage all of the equipment in the house from a distance by using one application. To implement the IOT as in the example above, many of the technologies involved include: RFID as a means of identification and object identifiers and location, web technology, near field communication, or wireless sensor network WSN (Wireless Sensor Network), and cloud computing. Technologies in
this IOT terminal connected to a variety of data collection through the Internet and other communication networks. Information on the environment around the object captured in real time, and then converted into a data format suitable for transmission over the network, and is sent to the data center. The data is then processed by the processor intelligently using cloud computing and other smart computing technology that can process large amounts of data, to achieve the purpose of the IOT. many technologies involved include: RFID as a means of identification and object identifiers and location, web technology, near field communication, or wireless sensor network WSN (Wireless Sensor Network), and cloud computing. Technologies in this IOT terminal connected to a variety of data collection through the Internet and other communication networks. Information on the environment around the object captured in real time, and then converted into a data format suitable for transmission over the network, and is sent to the data center. The data is then processed by the processor intelligently using cloud computing and other smart computing technology that can process large amounts of data, to achieve the purpose of the IOT. many technologies involved include: RFID as a means of identification and object identifiers and location, web technology, near field communication, or wireless sensor network WSN (Wireless Sensor Network), and cloud computing. Technologies in this IOT terminal connected to a variety of data collection through the Internet and other communication networks. Information on the environment around the object captured in real time, and then converted into a data format suitable for transmission over the network, and is sent to the data center. The data is then processed by the processor intelligently using cloud computing and other smart computing technology that can process large amounts of data, to achieve the purpose of the IOT. near field communication, or wireless sensor network WSN (Wireless Sensor Network), and cloud computing. Technologies in this IOT terminal connected to a variety of data collection through the Internet and other communication networks. Information on the environment around the object captured in real time, and then converted into a data format suitable for transmission over the network, and is sent to the data center. The data is then processed by the processor intelligently using cloud computing and other smart computing technology that can process large amounts of data, to achieve the purpose of the IOT. Technologies in this IOT terminal connected to a variety of data collection through the Internet and other communication networks. Information on the environment around the object captured in real time, and then converted into a data format suitable for transmission over the network, and is sent to the data center. The data is then processed by the processor intelligently using cloud computing and other smart computing technology that can process large amounts of data, to achieve the purpose of the IOT. Technologies in this IOT terminal connected to a variety of data collection through the Internet and other communication networks. Information on the environment around the object captured in real time, and then converted into a data format suitable for transmission over the network, and is sent to the data center. The data is then processed by the processor intelligently using cloud computing and other smart computing technology that can process large amounts of data, to achieve the purpose of the IOT.

3. Methodology Of Research

3.1. Analysis Tool IOT system works

Learn how to work the system device IOT of the SSL configuration, log into the system IOT until the delivery of data to the server.

3.2. Data Collection

Collecting data on the configuration and the type of device IOT -type
3.3. Conduct Implementation OTP

OTP devices perform application of IOT with images contained in the figure below:

![OTP Diagram](https://example.com/otp-diagram.png)

Figure 1. IOT configuration

The explanation of How to Work System, The first user to register the device IOT platform to that which already contain Id IOT device, which registered are the IOT Device id, and platform into database checks whether it is valid, if valid, the IOT platform will send the OTP code for access to the device IOT, after getting OTP code then the user enters the code so can IOT device is accessed. Scenarios to -2. IOT device has its own GSM module for SMS receive so the user does not need to enter a code OTP.

4. Conclusion

IoT devices need to be enhanced by using One Time Password to protect data and exploit IoT devices by unauthorized people.

In the future, the IoT device features a GSM Module for automating requests and input One Time Password codes to facilitate the authentication process. The data used in this study is the data of Coal Exports In Indonesia by the main destination countries in 2006-2015 (can be seen in Table 1). Data Processed from customs documents of the Directorate General of Customs and Excise quoted from the Publication of Statistics Indonesia.

References

[1] N. Haller et al, "A One-Time Password System", RFC 2289, February 1998. [Online]. Accessed on: https://tools.ietf.org/rfc/rfc2289.txt
[2] Leslie Lamport, "Password Authentication with Insecure Communication", Communications of the ACM 24.11 (November 1981), 770-772
[3] RL Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key cryptosystems", Communications of the ACM, V.21 n.2, p.120-126, Feb. 1978 [doi>10.1145 / 359340.359342]
[4] C. Qiang, G. Quan, B. Yu, L. Yang, "Research on National Security Seminar and Expo 2015 89 Electrical Engineering ISSN: 2088-9984 Issues of the Internet of Things", International Journal of Future Generation Communication and Networking, 2013, Vol.6, No.6, pp.1-10
[5] A. Wanto. M. Zarlis. Sawaluddin. and D. Hartama. “Analysis of Artificial Neural Network Backpropagation Using Conjugate Gradient Fletcher Reeves in the Predicting Process.” Journal of Physics: Conference Series. vol. 930. no. 1. pp. 1–7. 2017
[6] R. Roman, J. Zhou, J. Lopez, On the Features and Challenges of Distributed Security and
Privacy in the Internet of Things, Computer Network Journal, Elsevier, 2013

[7] CM Medaglia, A. Serbanati, D. Giusto et al. (Eds.), "An Overview of Privacy and Security Issues in the Internet of Things", 20th Tyrrhenian Workshop on Digital Communications, Springer Science + Business Media, LLC 2010

[8] European Lighthouse Project, "Introduction to Architectural Reference Model for the Internet of Things Booklet", 2013.

[9] M. Sharifnejad, Shari M., M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT 2007.

[10] T. Borgohain, U. Kumar, S. Sanyal, Survey of Security and Privacy Issues of Internet of Things.2015, http://arxiv.org/abs/1501.02211 [11] S. Gildiyal, A.