Jurnal Elektronik Ilmu Komputer Udayana
Volume 8, No 4. May 2020

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Data Communication Security Design on IoT Based Systems with the Port Knocking Method

I Made Andre Dwi Putra[a1], I Komang Ari Mogi[a2]

[a]Informatics Engineering, Faculty of Math and Science, University of Udayana
South Kuta, Badung, Bali, Indonesia
[1]andredwiputra0413@gmail.com
[2]arimogi@gmail.com

Abstract

Technology is a familiar thing among the people and the internet is something that is always used in everyday life to help with work. With technology and the internet, IoT (internet of things) can be realized in every device available to build a Smart City. However, there are still people who use the internet to commit crimes. To prevent it is not enough with a firewall, there needs to be a more security system. In this article, discussing how to tap on a port will be able to help manage the IoT-based system. The success rate of previous studies that support SSH by using port knocking is very good but in the author's study only to the design design only.

Keywords: *IoT, Smart City, Firewall, Port Knocking, Internet, Port*

1. Introduction

The number of crimes that occur on the internet that causes unrest in internet users because their data is very confidential can be seen by someone. So the internet network must contain a high security as it is known that security on the internet network is still so minimal that hackers can hijack a system and retrieve existing user data. As an example of the problems that exist on Facebook that he said many Facebook user data has been hijacked. Therefore this article was made in order to improve security on the internet network [1].

IoT (Internet of Things) is an ability to connect smart objects and enable them to interact with other objects, the environment and other intelligent computing equipment connected to the internet. Many cities and tools have implemented IoT. By connecting various objects that are connected to the internet that causes the internet network to be open and can make it easier for hackers to enter and retrieve existing data, it requires a high level of security so that data is being transmitted on an IoT-based system. cannot be hijacked or manipulated. Because of the importance of user data privacy for the user itself [2].

In the survey, it is said that security on the device can still be manipulated by intruders which, for example, a surveillance camera that wants to send data to the server but the port on the surveillance camera is tracked by someone who is not responsible then the device can be reprogrammed by someone and the data which will be sent can be sent to the server of someone who is not responsible is not sent to the original server

The case that can occur is if the user is using wifi in public places, then the things done by the user can be recorded, and also the data sent can be sniffed by someone using wireshark tools, and someone can also hack the user because the port will continue open.

The Port Knocking method is a method for securing a port so that it is not freely entered by people. This Port Knocking method can be likened to someone who wants to enter the house using the knock conditions, if the knock is wrong it will not be allowed to enter. The one who controls the knock on this method is the user who created the system. This knock can be said to be the key to enter this port. By using this method it is expected that the data communication process that occurs on an IoT-based system will be safe [3].

In this study the authors used the Port Knocking method. The Port Knocking method is a method for securing the port to be accessed so that not just any user can access the port.

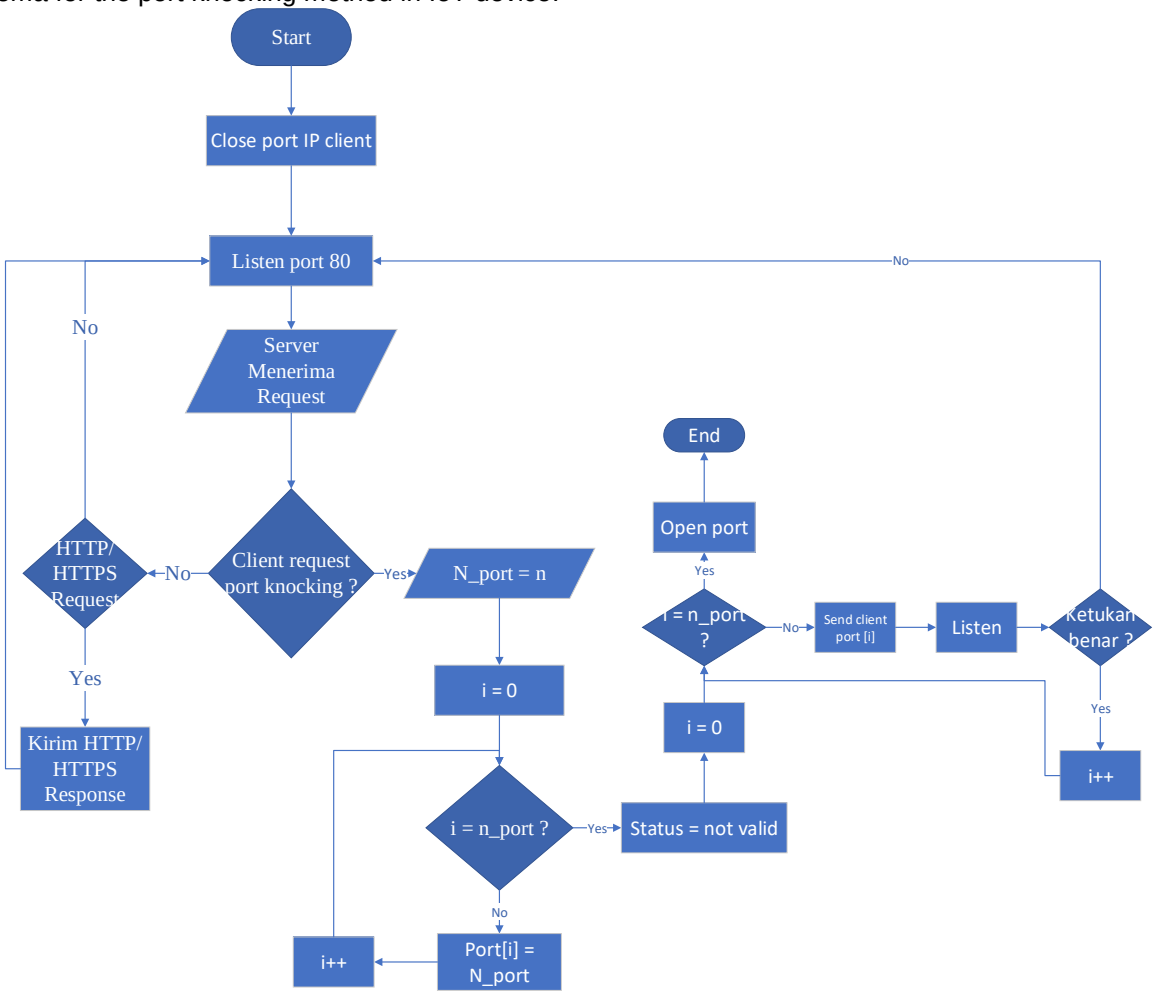
In a previous study (Rometdo Muzawi, 2016) utilizing the port knocking method was said to be able to optimize the internet network security system.

In previous studies using the port knocking method by collaborating with a firewall to protect the proxy as an authentication security system on a network service server and to secure a server from 3 attacks namely Hydra, DoS, and Telnet using TCP protocol [4].

In the previous research, it was explained how the implementation of simple port knocking aims to close the gap on the server side by making the port on the router invisible to other parties that are not trusted even though it has been scanned, but will still look open and can be accessed by parties that have been authenticated so as to prevent attack access from the attacker [5].

2. Reseach Methods

In this study the method used is the Port Knocking method as follows.
Previously gave an address to a firewall like iptabels. The knocking port usually requires 2 or more ports that can be allocated to monitor beats [6]. Knocking or knocking is determined from the start.
Schema for the port knocking method in IoT device:



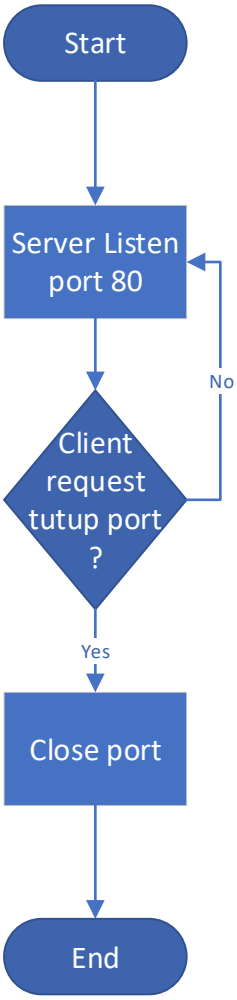
Picture 1. Schematic for port knocking in IoT devices to open

1. The IoT device here can be said as a server. First it will close the port on a particular IP client to open the port.
2. The IoT device is in the listen condition to be ready to receive input from the client.
3. The IoT device accepts port knocking requests from the client and is tested whether the received request is for port knocking or HTTP / HTTPS requests.
4. If an HTTP / HTTPS request is received, the HTTP / HTTPS response is sent by the IoT device to the client and returns to the listen state.
5. If so, the server initializes n_port = n.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

6. Then process i = 0.
7. Then enter the process of storing the ports to be tapped on the array as many rules as specified
8. The status on the IoT device is still not valid because the tapping process has not yet occurred.
9. Process i = 0.
10. Enter the port tapping condition, is i = n_port? if not, then the port in the array in index i is sent to the client.
11. The server returns to the listen state.
12. If the knock is correct then the tapping process will repeat as many ports as there are in the array in index i.
13. If not, the IoT device sends a status not valid to the client and returns to the listen port 80 state.
14. If yes I = n_port then the destination port is open.

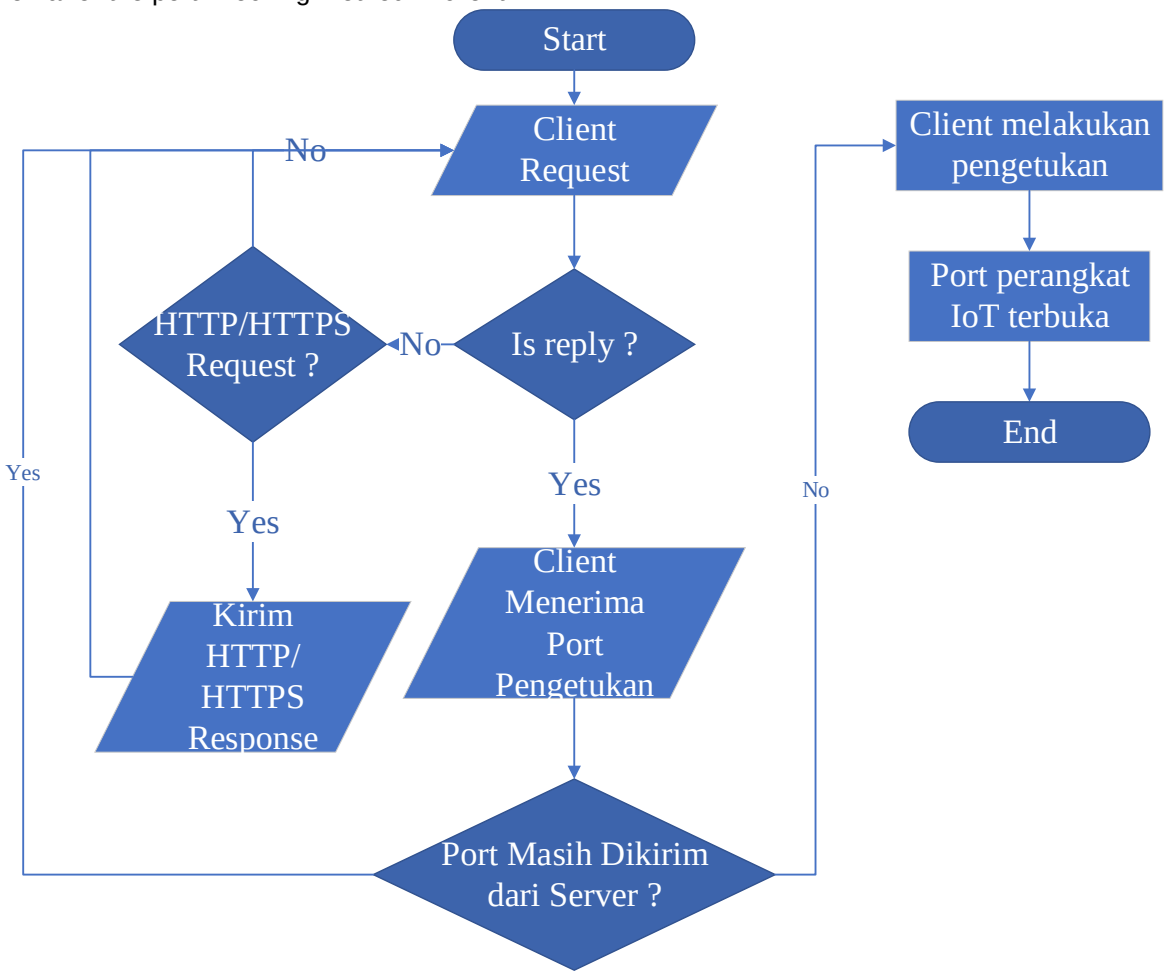
Schema to close the port on the server (IoT) :



Picture 2. Schematic for port knocking in server to close

Explanation:
1. When closing a port, the server is listening
2. The IoT device is ready to accept the closing port request from the client.
3. If the IoT device accepts, the port will be closed, and if not, it returns to the listening state.

Schema for the port knocking method in client :



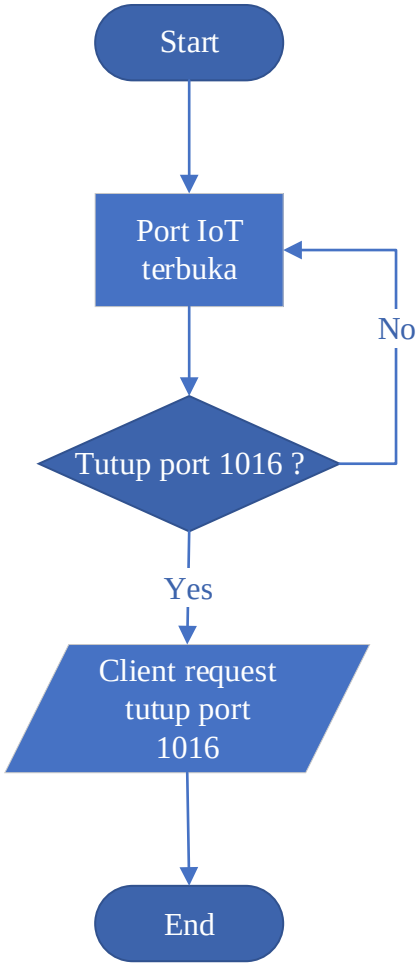
Picture 3. Schematic for port knocking in client

Explanation :

1. In the first process the client will request to the server.
2. If yes, the client receives a port.
3. If not what is HTTP / HTTPS request?
4. If an HTTP / HTTPS request is received, if yes, the HTTP / HTTPS response is received and returned to the client request.
5. If not, then return directly to the client request.
6. If the client has received the port to be tapped, it enters the tapping process.
7. If the tap is correct then the client will receive a valid status from the server and if it does not return to the client request.
8. Is the port still being sent? If it does, the port request process will continue to repeat until the port sent by the server runs out and if not, the IoT port will open.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

The scheme closes the port on the client



Picture 4. Schematic of closing ports on the client

Explanation:

1. The IoT port is still open, and the client wants to close port 1016.
2. If yes, then the client requests the server to close port 1016 and if not, port 1016 remains open.
3. Done

3. Result and Discussion

The results obtained are the design of a security system on the IoT port that uses the Port Knocking method to secure the port. The testing will be done using a virtual machine which in the virtual machine will be simulated using a client and server (the server is IoT). After that, it will be seen how successful it is in securing its IoT port. Because this research only reaches the design of the system flow. Ports in this study can be used by any port, but the author here exemplifies port 1016.

4. Conclusion

The conclusion is that this port knocking method is able to help protect port 1016 that has been protected by a previous firewall to block users who want to enter the port by force. Because the port knocking method has previously been used in studies that have been there before to protect attacks from hackers. Schema or plot of using this port knocking method as in the results and discussion. Hopefully with this design the authors can implement later and can take advantage to realize a safe Smart City.

References

[1] Bertino, Elisa and Choo, Kim-Kwang Raymond and Georgakopolous, Dimitrios and Nepal, Surya "Internet of things (iot): Smart and secure service delivery" *ACM Transactions on Internet Technology (TOIT),* vol. 16, no. 4, p. 22, 2016.

[2] Arasteh, H and Hosseinnezhad, V and Loia, V and Tommasetti, A and Troisi, O and Shafie-Khah, M and Siano, P "Iot-based smart cities: a survey" *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC),* p. 1-6, 2016.
[3] Amarudin, Amarudin " Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking" *Jurnal Teknoinfo,* vol. 12, no. 2, p. 72-75, 2018.
[4] Suchendra, Devie Ryana and Rahman, Alfian Fitra and Ismail, Setia Juli Irzal " PENERAPAN SISTEM PENGAMANAN PORT PADA LAYANAN JARINGAN MENGGUNAKAN PORT KNOCKING" *Jurnal Komputer Bisnis,* vol. 10, no. 2, 2017.
[5] Kusuma, Aprianto Puji Adi "Implementasi Simple Port Knocking pada Dynamic Routing (OSPF) menggunakan Simulasi GNS3" *Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya,* 2016.
[6] Krzywinski, Martin " Port knocking from the inside out" *SysAdmin Magazine,* vol. 12, no. 6, p. 12-17, 2003.
[7] Muzawi, Rometdo " Aplikasi Pengendalian Port dengan Utilitas Port Knocking untuk Optimalisasi Sistem Keamanan Jaringan Komputer" *SATIN-Sains dan Teknologi Informasi,* vol. 2, no. 1, p. 52-58, 2016.