International Journal of Engineering & Technology, 7 (4.4) (2018) 3-4

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Study on Lightweight Cryptography Algorithm for IoT based Bicycle Sharing System

Larsson Bajracharya 1, JongmunJeong 2, Mintae Hwang 3*

[1]*Dept. of Eco-Friendly Offshore Plant FEED Engineering, Changwon National University, 20 Uichang-gu Changwon-si 51140, Korea*
[2]*Dept. of Information and Communication Engineering, Changwon National University, 20 Uichang-gu Changwon-si 51140, Korea*

Abstract

In this paper, we studied lightweight cryptography for IoT based Bicycle Sharing System. We maintained a remotely located real time server and four separate stations with kiosk control box system, designed with Internet based IoT devices. Then, we calculated the processing time to unlock the bicycle from each station, once the request was sent to the server. The calculated load and processing time were compared after the application of cryptography algorithm. The comparison helped us conclude that the LEA cryptography showed minimal time difference when applied in a real time system. At the same time, highly secure data transmission was also achieved.

Keywords: lock, encryption, IoT, cryptography, source code

1. Introduction

IoT (Internet of Things) has been recognized as the area with high number of research and future possibilities. The number of devices being used have been increasing since 2009. However, in the past decade IoT has been covering wide range of applications like healthcare, utility, transport etc [1]. With the introduction of IoT in larger scale, many security issues have been recorded. These existing IoT systems must maintain strong security, minimized control of humans, and strong resistance to the environment [2]. However, there is an increasing number of attacks targeted at Internet of Things every year [3]. Cryptography is a viable option when it comes to the security of an IoT based system. As the IoT devices at end users have low power and performance, IoT should consider using lightweight cryptography to minimize resource consumption [4]. As bicycle sharing system is a widely used commercial transportation system [5], testing an encryption algorithm in such system is more practical. Therefore, we built an IoT based bicycle sharing system and studied the time consumed while sending a request to the server from these stations, before and after the application of LEA (Lightweight Encryption Algorithm) cryptography algorithm. LEA was preferred over other algorithms because of its high speed and high security against attacks on block ciphers.

2. Architecture of the System

Fig. 1 shows the architecture of the bicycle share system implementing LEA cryptography. A mobile application is used to request for access code for bicycle unlock. Each station consists of docks to park bikes along with a control box consisting of IoT devices as well as an LTE (Long Term Evolution) modem to connect to remote server via internet. The encryption algorithm implemented in the control box encrypts the access code entered by the user when sending to the server as well as decrypts the response data received from the server.

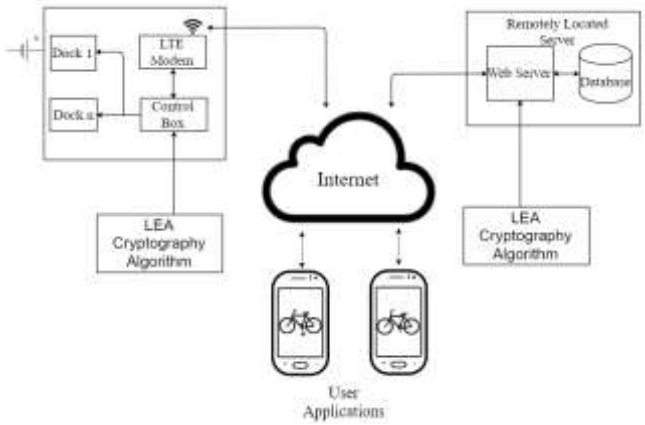

Figure 1:. Architecture of the IoT based bicycle share system implementing Cryptography.

3. System and Performance Comparison

Both the systems with and without LEA cryptography used the same hardware configuration. However, the source code for the systems were different. All the codes were written in PHP and Python programming language in an IDE (Intelligent Development Environment).

3.1 Source Code

Table 1, below shows the comparison between source codes before and after the LEA encryption algorithm in the station control box.

Without LEA Encryption	With LEA Encryption
passwd = textlist[1:5] password = ".join(passwd)	**key = bytearray(b"16 24 or 32 bit key")**

Without LEA Encryption	With LEA Encryption
station = textlist[5:-2] stat = ''.join(station) query_args = {'pass': pass-word,'station': stat} query_stat = {'stat': stat} encoded_args = url-lib.urlencode(query_args) encoded_stat = url-lib.urlencode(query_stat) url = 'serverloca-tion/bicycle/passwordcheckborrow.php?' + encoded_args req = urllib2.Request(url) response = urllib2.urlopen(req) result = response.read() url2 = 'serverloca-tion/bicycle/passwordverifyborrow.php?' + encoded_stat req2 = urllib2.Request(url2) response2 = urllib2.urlopen(req2) result2 = response2.read()	passwd = textlist[1:5] password = ''.join(passwd) **enc = bytearray(password, "utf8")** **leaECB = LEA.ECB(True, key, True)** **encpassword = le-aECB.update(enc)** **encpassword += leaECB.final()** station = textlist[5:-2] stat = ''.join(station) query_args = {'pass': **encpass-word**,'station': stat} query_stat = {'stat': stat} encoded_args = url-lib.urlencode(query_args) encoded_stat = url-lib.urlencode(query_stat) url = 'serverloca-tion/bicycle/passwordcheckborrow.php?' + encoded_args req = urllib2.Request(url) response = urllib2.urlopen(req) result = response.read() url2 = 'serverloca-tion/bicycle/passwordverifyborrow.php?' + encoded_stat req2 = urllib2.Request(url2) response2 = urllib2.urlopen(req2) result2 = response2.read()

3.2 System Performance

The performance evaluation of the system was done before and after the encryption algorithm was placed in the station and server.We calculated the time taken for communication between station and server. In case of study with the encryption algorithm, the total time was calculated between data encryption with LEA in the station, transmission of the encrypted data and then decrypting the data in the main remote server. To measure the performance, we maintained four stations along with control boxes. A trial of 50 times were performed-for each of these stations simultaneously to send the data to the server. A MySQL database was maintained inside the control box to record the time difference between data sent and received by each station. Fig 2. below shows the graph comparing average time required by the stations for successful communication and data transmission, before and after the encryption algorithm.

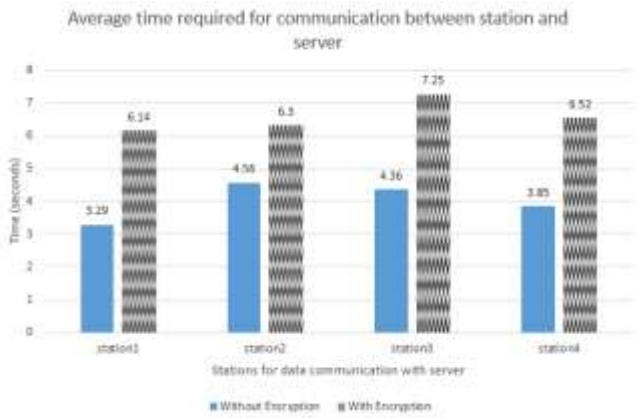

Figure 2:. Evaluation and comparison of average time required for communication between stations and server.

4. Conclusion

In this paper, we studied the performance of an IoT based Bicycle Sharing system with and without the use of a LEA. We found out that the time difference between bicycle request and retrieval was minimal even when the tests were performed simultaneously and the system ran through an extra layer of encryption algorithm.

Acknowledgment

This paper was supported by Changwon National UniversityResearch Fund in 2017

References

[1] Jayavardhana Gubbi, MarimuthuPalaniswami, Rajkumar Buyya and Slaven Marusic, On Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems. 29 (2013), 1645–1660.

[2] Hyun Soo Chang, Kim hyeonjin and Taeshik Shon. On A Study on Cyber Security Issues in Industrial IoT Environment, REVIEW OF KIISC. 25.5 (2015): 12-17.

[3] Denis Makrushin, Igor Grachev, Mikhail Kuzin, Vladimir Kuskov and YaroslavShmelev, On Honeypots and the Internet of Things [Online], (2017). Available:https://securelist.com/honeypots-and-the-internet-of-things/78751/

[4] Ko Yun Seung, On Study of Policies of Major Countries on Internet of Things and Market Forecast, International Commerce and Information Review. 16.5 (2014), 27-47.

[5] J. Cheshire, M. Batty and O. O'Brien, On Mining bicycle sharing data for generating insights into sustainable transport systems, Journal of Transport Geography. 34 (2014): 262-273.