Automatic Toll Road Payment System Security Using Radio Frequency Identification (RFID) with the Blowfish method

To cite this article: Ahmad Fali Oklilas et al 2019 J. Phys.: Conf. Ser. 1196 012008

View the article online for updates and enhancements.
Automatic Toll Road Payment System Security Using Radio Frequency Identification (RFID) with the Blowfish method

Ahmad Fali Oklilas*, Fitriyani, Ahmad Zarkasi

Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya, Indonesia

*fali@ilkom.unsri.ac.id

Abstract. This paper makes the toll road payment system automatically using Radio Frequency Identification (RFID) using the Blowfish method. RFID will be applied to toll road payment system aims to be able to identify objects quickly, so that will provide time efficiency and will realize a new revolution in payment management. In applying for the payment automatically is necessary accuracy and speed for the introduction of the object. So by using such a system is expected to reduce the congestion that often occurs in front of toll doors and toll road exit. This is usually due to the length of time spent on manual payment transactions at the toll gate, where using a manual payment system can make the toll road service limited efficient and less satisfactory. In addition to the speed of transaction time in the toll door, data security is also required from the device used by the user i.e. electronic card toll or e-toll using RFID tags. E-toll card data theft will harm the user. The blowfish method here is used to secure or conceal user data, so securing user data can prevent manipulation from occurring to duplicate RFID tags.

1. Introduction
Radio Frequency Identification or better known as RFID is a technology that the process does not require direct contact with humans, usually the process is done by using radio frequencies that will be used to achieve identification automatically. RFID is also called the auto-ID method that normally uses radio waves. In such systems, there is usually a tag and reader that will be used for RFID system processing. In order for the tag to be executed when the tag should be close to the RFID reader and the reader will identify data based on the data or information contained in the RFID tag. RFID tags are usually shaped by various kinds of cards, stickers and many other forms. Each tag has a unique data ID that makes the data ID different each tag [1].

RFID usually consists of tags, readers and host systems. RFID communicates wirelessly so as to identify an object or person using a device called a tag. Contact between RFID tag with the reader cannot be done directly but by way of sending the electromagnetic wave. RFID can also be referred to as a technique that uses radio waves to obtain identity objects. So, this is what makes RFID can make a transaction or process automatically. RFID is famous for its ease of detecting an item and can also be used in the payment process [2].

But behind the ease with which it offers there is a problem that arises in this system is the problem in terms of security that must be overcome. Usually, a very important security problem to be addressed in the RFID tag section. RFID tags can be copied by eavesdroppers if there is no security system. If the attacker manages to retrieve the data contained in the tag then they can create a duplicate tag for the RFID tag card that will be used in the toll payment system [3].

Therefore, in a toll road payment system using RFID will be applied with a cryptographic algorithm. This cryptography is an algorithm that is often used to secure data or files, keeping important
information and maintaining it privately. Cryptography will make the message to be sent cannot be understood by others. So the message to be sent cannot be understood by the attacker. Therefore, in this paper using the Blowfish algorithm. The function of the Blowfish algorithm in this paper is to secure the data contained in the tag. This Blowfish algorithm is a symmetric key that is in the form of a block cipher. How to calculate using block cheaper. In this Blowfish algorithm, there is an encryption process that will make the data not understood by the attacker. Encryption is the process of altering the original data or that is usually called the plaintext so that the data cannot be read or understood its meaning. In the Blowfish algorithm, the symmetry key used is a cypher block that will perform plaintext and ciphertext processes in the form of blocks that are divided into bits [4].

Actually, the use of Blowfish method in this toll road payment system is to secure the data that is on the RFID Tag. Indeed the RFID tag has memory used to store data in a small switch. The reason why the data in the tag needs to be secured is that RFID tags are very vulnerable to cloning attacks. This cloning attack can carry out attacks when the data will be sent to the server by using a local host so this cloning attack will see the original RFID tag id and after that the attacker will duplicate the card by copying the original RFID ID tag to the RFID tag that is still empty by pasting the data in the original RFID tag. So the card that is duplicated will be very similar to the original [4].

2. Related work
In the previous review literature, whereby papers implicate the security of RFID tag data transmission using the DES cryptography method. This process to maintain data security when the data transmission process takes place. Then the RFID tag ID must be encrypted first with this DES method. This DES method will modify the RFID 8-bit tag ID and will also be added with the user password of 8 bits. So the data will be 16 bits and can be applied with a DES algorithm. DES algorithm is actually almost the same as Blowfish because both cryptographic systems are symmetry type which also types cypher block. DES data algorithm is only 64-bit size. DES will convert 64 bits of plaintext data to 64 bits of ciphertext based on 56 bits of the internal key. The general process of the DES algorithm is that the plaintext block formed in the initial permutation position will then be encrypted 16 times round by using different keys in each encryption process. Furthermore, the result of the encrypted data is reshaped its position based on the inverse table of the initial permutation into the data that has been encrypted. If this algorithm is applied to the toll road payment system is inefficient because the DES algorithm includes a long cryptographic algorithm with a key of only 64 bits so that in the security of the RFID tag ID is still less secure than the new cryptography [5].

Therefore, in this paper, the authors use the Blowfish algorithm because the Blowfish algorithm can reach 448 bits long so it will make the data very long and complicated which will make the data difficult to understand. The Blowfish algorithm generally has the first two parts: the key expansion and the second the data encryption. The data encryption process in the Blowfish algorithm consists of 18 rounds in which each round there are key-dependent and substitution keys. All the process of operation is XOR with variable must be 32-bit, addition and mod operation. In the Blowfish encryption process to determine the plaintext blocks it takes 64 bits then the input value is 64 bits and the output is 64 bits. For the key capabilities of the Blowfish algorithm varies there are ranges of only 32 bits, but the maximum limit to 448 bits. So, the greater the capacity it will make the greater the security capacity. The description process of the Blowfish algorithm is the reverse of the encryption process so in the calculation the encryption process starts from finding p1 for the description starting from 16 so that the subkey is also used in reverse order [6].

3. Materials

3.1. Tag radio frequency identification
This RFID tag is a tool that will be used as transmission equipment or also often called a transponder that is enabled to hold data transmitted to the reader when receiving a request from the reader. RFID tags generally consist of three kinds that each has its own task. First is the Integrated Circuit which is used as the place of command execution and data storage. The second is a coil or winding that functioned as a process of sending and receiving radio frequency waves. A third is the RFID tag usually there is
also a memory used to store data. Which data can be stored in the tag is only small. The memory contained in the RFID tag is divided into cells, so the cells will store data in the form of reading only and read-write. RFID tags are also divided into 3 types namely the first active tag, passive, and semi-passive which each type of tag has advantages and disadvantages of each [7].

3.2. Reader
Reader in the RFID system will be used as a modulation device and demodulate radio frequency signals that will make the reader able to communicate with the tags. Actually, the most important components in RFID systems are the reader and antenna tags. The reader is a device used to read the codes contained in the tag. Basically, the tag and reader system contained in RFID is divided into several types that can be used. The first type is the passive reader active tag (PRAT), the second is the active reader passive tag (ARPT) and the last active reader active tag or which can be abbreviated as ARAT [8].

3.3. Antenna
RFID has electromagnetic waves used for communication media. The antennas on the RFID are used as devices to transmit radio frequency signals between RFID reader and RFID Tag. The information contained in the encoded will enter the radio frequency wave through the transmission line, so the antenna has a very important role in the RFID system. In general, the types of antennas that are in RFID systems are also the same as antennas in general, such as Directional and Omnidirectional. Which directional antenna will send and receive radio signals in only one direction. While the omnidirectional antenna will send or receive radio signals from all directions simultaneously [9].

4. Research method
In the system design process consists of hardware design and application of blowfish algorithm that is enabled to secure data in RFID tags. In this sculpture will make this system must be able to read RFID tags. After the data is read, then the data will be encrypted and the next process should be able to receive data that has been decrypted. At the time of RFID tag reading process, a reader is an early stage in payment system of this toll road. In this paper, the author will use the RFID tag read and write or R / W. The reason why authors prefer RFID R / W tag is because in the process of paying the toll road requires money or can also use quotas. So the value of money is stored in RFID tags that will be used in toll road payment system. Once the user has paid automatic toll road payment the money value contained in the RFID tag will be reduced and when the user wants to recharge the RFID tags used in the automatic toll payment system the data in the RFID tag will change. So this is what makes the author in this paper using RFID tags Read / write. The data contained in the RFID tags that will be used in this toll road payment system only have ID number and amount of money. Because the RFID tag has a small memory then the data can be stored only the ID number and the amount of money. The ID number contained in the RFID tag is used as the key to open the activity during the transaction process is done and also to open the card owner's biography. Because RFID tags are only capable of storing multiple characters so that the full data is present on the server. After the transaction is done when the value of money or quota will be reduced so that the reader will rewrite the new data to the RFID tag.

In the process of data retrieval by the researchers then get the data or the value of the ID tag RFID is worth 16 hex. Which one to apply blowfish algorithm in toll road payment system automatically using RFID with blowfish algorithm required 64-bit binary. This is what makes the data needs to be modified first. The first thing that researchers should do before doing the calculations manually is the researcher must make RFID tags used by the author in conducting this research can issue ID. After the tag ID can be read by the reader then the hex tag-shaped ID is changed in the binary form first, Once it is divided into 32 bits. After that we initialize the first p-array in the form of hex then we must change first in binary form. To find the value of X, then we use formula $X_j = X_i \text{Xor} R_{P_i}$ after getting the result then we use the result to determine the value of S-box that will be used to find $X_R$ value. To find the value of $X_R$ then must use the formula $F(X_L) = ((S_1 + S_2 \text{mod } 2^{32}) \text{Xor} R_{S_3} + S_4 \text{mod } 2^{32})$.

The encryption process consists of the process input in the form of plaintext, then key entered, after that encryption process with Blowfish algorithm, generating ciphertext. As for the research steps, Blowfish algorithm is used with Flowchart of Key Encryption Processor ID as shown in Figure 1.
Figure 1. Flowchart of key encryption processor ID.

Figure 2. Manual Calculation Flowchart for Blowfish Algorithm.

Figure 2 describes the flowchart of the Blowfish algorithm calculation process manually. Where the initial value of the binary ID that consists of 64 bits is divided into two parts $X_L$ and $X_R$ consisting of each 32-bit binary number. Then XoR calculation is done for both using the formula $X_L = X_L \text{ XOR } P_i$ and $X_R = F(X_L) \text{ XOR } X_R$. The calculation is carried out iteration 16 times around. After 16 iterations, the formula for the 17th round is $X_R = X_R \text{ XOR } P_{17}$. Then the 18th calculation uses the formula $X_L = X_L \text{ XOR } P_{18}$. The results of both are Swap $X_L$ and $X_R$, as the end result is merged into 64 bits in binary form. For refinement, it converts to 16-bit hex in accordance with the initial 16-bit ID.

5. Result and analysis
Stages are done in the process of data retrieval is by first connecting the hardware used in this study is the reader with software, after that in the process of this study the author uses a USB port connected to
the computer. So in this study, the author will use port 8 and also by using one RFID tag with ID E191 8171 6DCB A000. The data is 16 bits and the frequency used in this RFID tag is 13.56 Mhz.

When the tag is placed or near the RC255 antenna the program will display the ID of the RFID Tag being used. The process of data retrieval conducted aims to test the process of data retrieval. In the process of retrieving this data is done by the reader that will read the ID tag RFID which will then be sent to the computer. The results of RFID Tag ID encryption calculations are as follows:

ID: E191 8171 6DCB A000

Binary: 11100001 10010001 10000001 01110001 01101101 11001011 10100000 00000000

X_L: 11100001 10010001 10000001 01110001 
X_R: 01101101 11001011 10100000 00000000

P_1 : 00100100 00111111 01101010 10001000

Where: X_L=the first 32-bit value of the binary number 64 original, X_R=the second 32-bit value of the binary 64 bit original, P_1=Blowfish algorithm P value array.

Then the process is done and finally get the following results:

Output (binner) = 00001111 10111110 00001000 00100111 11001101 11111001 
Output (hex) = OFBE 0413 CDF9 67E9

Based on the results of tests that have been done by the author that the RFID Tag ID that has been encrypted with Blowfish algorithm will be very difficult to read. Because the encoded RFID Tag ID will be longer than the original ID data. This will make the ID complex and difficult to read.

6. Conclusions
Blowfish algorithms can be used to secure RFID Tag IDs which are 16 bits in hex and have the ability to add keys so that the ID length is 64 bits in binary form. So that the data can be encrypted using the blowfish algorithm. This blowfish algorithm would be well suited for tag ID security. This is because the ID on the Tag must be secured so that the ID data cannot be read by hackers. If the Tag ID data does not have a security system, it will be very easy for hackers to make fake tags or duplicate them.

References
[1] K. Janeczek, “Microelectronics Reliability Reliability analysis of UHF RFID tags under long-term mechanical cycling,” Microelectron. Reliab., pp. 2–7, 2017.
[2] H. Jannati and B. Baharak, “Security analysis of an RFID tag search protocol,” Inf. Process. Lett., vol. 1, pp. 11–15, 2016.
[3] A. Noer, Z. B. Hasanuddin, and D. Djiamaluddin, “Implementation of RFID Based Raspberry Pi for User Authentication and Offline Intelligent Payment System,” pp. 251–255, 2017.
[4] T. Mahajan and S. Masih, “Enhancing Blowfish File Encryption Algorithm through Parallel Computing on GPU,” pp. 4–7, 2015.
[5] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” Procedia Comput. Sci., vol. 78, no. December 2015, pp. 617–624, 2016.
[6] V. Poonia, “Analysis of modified Blowfish Algorithm in different cases with various parameters,” pp. 5–9, 2015.
[7] F. Zhu, B. Xiao, J. Liu, B. Wang, Q. Pan, and L. J. Chen, “Exploring Tag Distribution in Multi-Reader RFID Systems,” IEEE Trans. Mob. Comput., vol. 16, no. 5, pp. 1300–1314, 2017.
[8] N. Gjeldum, M. Mladineo, M. Crnjac, I. Veza, and A. Aljinovic, “Performance analysis of the RFID system for optimal design of the intelligent assembly line in the learning factory,” Procedia Manuf., vol. 23, no. 2017, pp. 63–68, 2018.
[9] Y. Jiang, R. Zhang, W. Cheng, and W. Sun, “An Efficient Multi-channel Reader Collision Avoidance Protocol in RFID Systems,” no. Wcnc, 2016.