Implementation of Security in RFID Tag Data Transmissions with DES Cryptography

Ahmad Fali Oklilas
Dept. Computer Engineering
Faculty of Computer Science,
Universitas Sriwijaya
Indralaya, Indonesia
fali@ilkom.unsri.ac.id

Ahmad Heryanto
Dept. Computer Engineering
Faculty of Computer Science,
Universitas Sriwijaya
Indralaya, Indonesia
hery@unsri.ac.id

Anggoro Prasetyo
Dept. Computer Engineering
Faculty of Computer Science,
Universitas Sriwijaya
Indralaya, Indonesia
angga.destiny94@gmail.com

***Abstract*— One use of RFID is used as a user authentication tool that can provide more access to a system. Security is much needed on RFID. If authentication rights are misused for the wrong thing then it is very dangerous. The scheme used is to send RFID Tag ID data as a unique authentication code. RFID Tag ID will be sent from client to server using local network scale. RFID Tag ID data transmission can be done using wireless transmission media. When shipping the "bugs" can steal data with sniffing techniques. To minimize the risk of data theft can be applied data encryption method with DES algorithm. There will be a modified 8-bit RFID Tag ID which will add 8-bit user passwords. So 16 bit data can be processed with DES algorithm. With the data encryption at the time of delivery from client to server then data sent will be encrypted. So tappers can not misuse existing data.**

Keywords—RFID; sniffng; DES

I. Introduction

RFID itself can be more useful and includes many aspects of efficiency when combined on a computer network. With this combination then RFID can be useful in many systems. For example in the medical field [1] [2] and trade industry [3]. In IoT itself, the RFID system is utilized by 11% while the security field is 7% [4].

But not always the efficiency of a system there is no problem. Security issues are a major problem that will arise from this RFID system. A security issue arising from an RFID system is to duplicate RFID Tag IDs which can be done at a fast time [5]. One of the prevention and handling of data security in RFID is by applying cryptographic method in the system. [illegible] original data will be hidden. So that if a thief managed to steal data on the way, of course the data obtained is not the original data from the data. Without any security in data transmission, many problems will arise [6].

In the application of data sender in two-way half-duplex using wireless media known term socket programming or that can be called socket programming. The sockets themselves can facilitate IPC or Inter Process Communication for applications running on the network [7]. Serves to create connections between client and server, after they are connected then can exchange messages. However, in the application of socket programming is not equipped with data security so that the need for data security techniques applied [8]. One of the techniques that can be applied is cryptography [9].

In cryptography itself there are many kinds of algorithms that can be used in data security. One of them is DES (Data Encryption Standart) [10]. By implementing the DES algorithm, RFID tag data will be safer when the Tag ID is sent to the server [11].

The data security mechanism on RFID tags will be sent from client to server using wireless transmission medium with local network scale [12]. In this thesis research, researching about data security, RFID security mechanism on sending tag data using DES. The scheme used in RFID data transmission is using cryptographic and DES algorithms.

II. Study of Literature

A. RFID (Radio Frequency Identification)

RFID itself is an auto-ID medote using radio wave media. In processing the RFID system itself consists of tags and readers. Where RFID tags will be placed adjacent to the RFID reader. The reader will then identify the data with the data contained in the Tag. RFID tag itself can be in the form of cards, stickers or other forms. Each Tag has unique ID data so that the ID data is one and the other is different. [14]

The RFID tag itself is often used instead of barcodes. RFID tags can be used without any direct contact. Because it has more favorable RFID memory [illegible] some information. RFID also has anti-collision capability that is the ability to read tags in many and fast ones. [16]

In this research mengugunkan 2 types of passive tags. Tags used are passive read only tags and passive read write tags.

Passive read only tags can only be read by the reader and can not be changed data. While passive tag read and write, the data on the tags can be modified and read by the reader.

Reader is a tool used to read the codes contained in the tag. Generally, based on tags and reader systems used RFID systems can be grouped as follows: Passive Reader Active Tag (PRAT), Active Reader Passive Tag (ARPT), and Active Reader Active Tag (ARAT).

The ARPT system consists of an active reader that sends out a check signal and also receives an authenticity response signal from a passive tag. The ARPT system uses passive tag generated by the checker's signal from the active reader. Jangakauan ARPT systems are usually relatively close ranging from 0 - 4 Cm, so usually ARPT systems are used in access control systems where Tags and Reader are close together for use.

B. DES Cryptography

DES cryptography itself belongs to the type of symmetry cryptography system type cipher block. DES is circulated on 64 bit blocks of data. DES converts 64 bits of plaintext data into 64 bits of ciphertext based on 56 bits of internal key. The internal key itself is built from an initial external key consisting of 64 bits of data. The general process of the DES algorithm is the plaintext block in its position based on the position with the initial permutation table. The result of the initial permutation position is then encrypted for 16 times by using different keys in each of the execution process. Then the result of the encryption is reshaped its position based on the inverse table of the initial permutation into the encrypted data. [11]

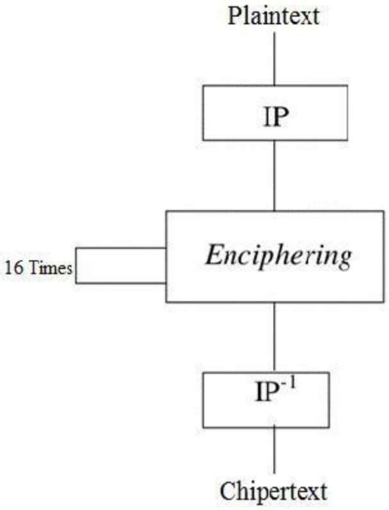


Fig. 2. Global Skema Algoritma DES[11]

In the encryption process, the blocks are divided into two sides of the section, the L side is the left side and the R side is the right side, each side consists of 32 bits. Both sides of this data are processed 16 times round DES. In each round, side data is used as a transformation function. During the transformation process, right-side data and internal keys are used. The output of the transformation process is then performed by calculating the XOR logic gate with the left side block to produce the new right side block. While the new left side of the block from the side of the previous block R.

C. Socket Programming

Sockets is a facility of Inter Process Communication (IPC) used in building computer network applications. To be able to communicate, the socket requires a unique address to function as identification. The identification of addresses consists of IP Address and Port Number. So Socket Programming is a program or application designed using socket communication. In socket programming is generally used to build communication programs and data transmission between two or more computers. Example is a client-server application model. Here is an overview of the socket program with a

client-server application model that uses the TCP protocol. [7]

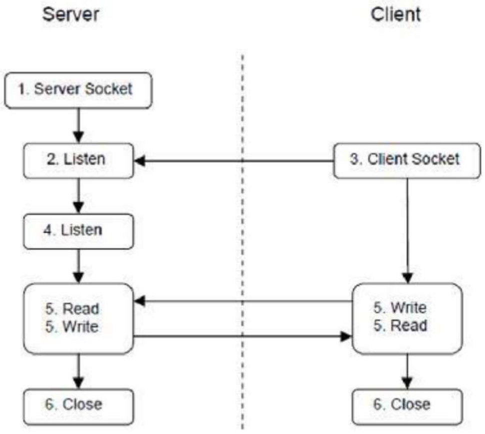


Fig. 3. Aplication Model Clien/Server in TCP Protocol[8]

III. METHODOLOGY

A. Initialize Network Scale and Hardware Design

This security system is applied on both sides of the workstation where each one plays a role as a reader or acts as a server. The process of sending data can be done after the hardware and software connected. The author will use RFC Reader RC-522 which is used to read or get the data value of ID from RFID Tag. This type of reader can not function as reader in general. To be able to make the reader work properly it needs hardware assembly assisted with arduino uno microcontroller as main processor. Here is a picture of Reader RFID RC-522 with Arduino Uno. [13]

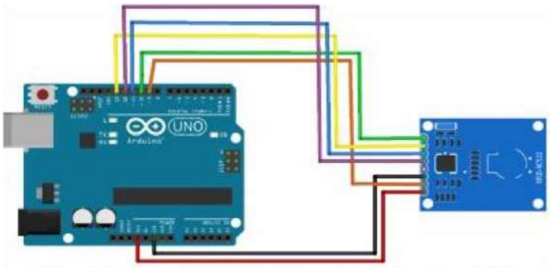


Fig. 4. Reader RFID RC-522 and Arduino Uno [13]

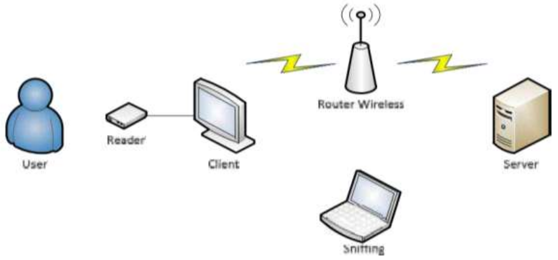


Fig. 5. Hardware Structure of RFID Tag ID Security System

B. Socket Program Design

Socket program is a program that is needed in this research. Where the socket program serves as an intermediary between the reader and the server. Simply this program is enabled to give way data that will run from the beginning of data reader reader until data accepted by server as final destination data. Client program serves as the program that will be addressed first by RFID Tag ID data. This program will send data reader reader to server. The Server program functions as the receiver of the RFID Tag ID data sent by the client.

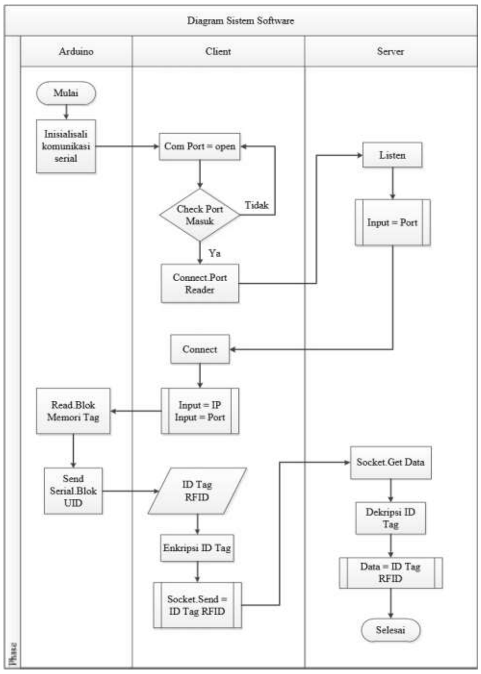


Fig. 6. software design diagram

C. System Design and Application of DES In Application Design

In the design of systems consisting of the design of hardware and software tools on the security system of delivery RFID tags are simulated on two different computers on a network. The system should be able to read the RFID Tag ID then send the encrypted data and be able to receive decrypted data.

Here is a design program Flowchart RFID Tag ID security application.

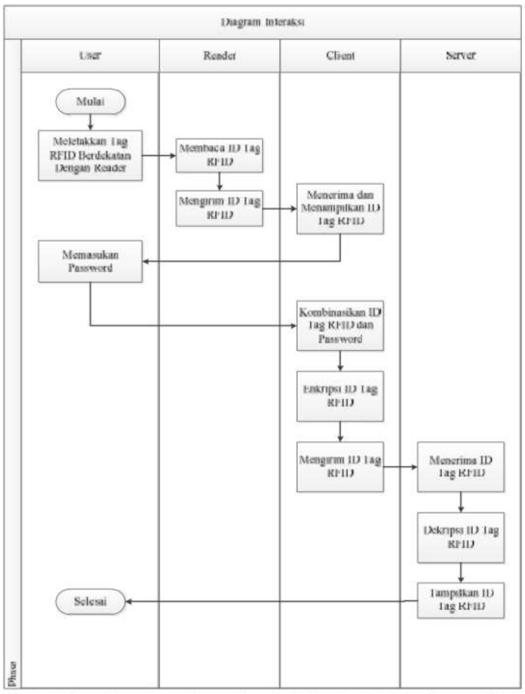


Fig. 7. Flowchart Design of RFID Tag ID Security application

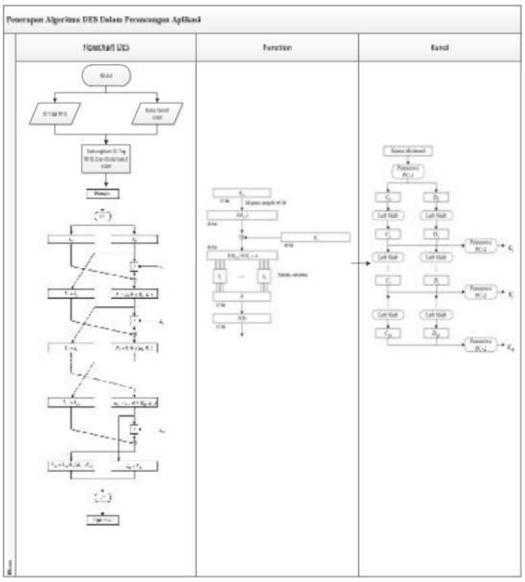
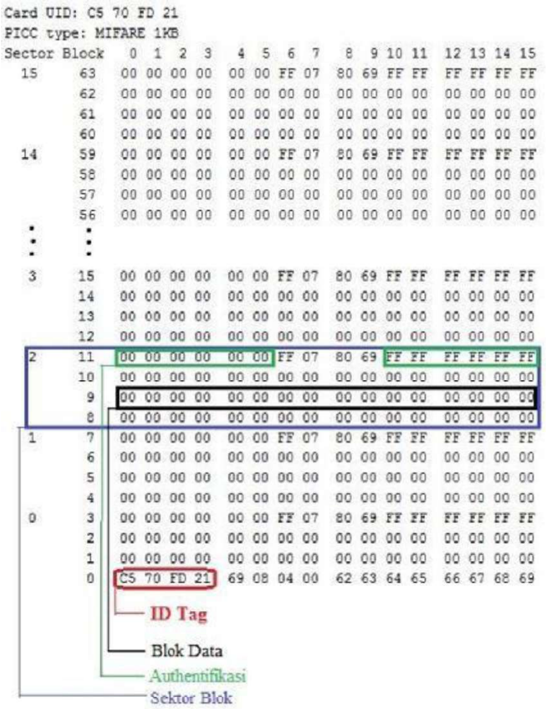


Fig. 8. Flowchart Application of DES Algorithm In Application Design

IV. RESULT AND ANALYSIS

The RFID Tag ID sending security system includes the process of reading and getting the RFID Tag ID by the reader and sending the data from the client computer to the server computer. In the final task of Visual Basic programming language used to build the system. The IDID tag ID data retrieval process is done using RFC Type RC255 Reader with 13.56 Mhz frequency. As previously mentioned each RFID tag has unique code or different IDs in each Tag. In this process the data will be read by the reader so that the data can be processed for the next stage.



```
Card UID: C5 70 FD 21
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15
  15     63   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF
         62   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
         61   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
         60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
  14     59   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF
         58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
         57   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
         56   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
   :      :
   3     15   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF
         14   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
         13   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
         12   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
   2     11   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF
         10   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
          9   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
          8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
   1      7   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF
          6   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
          5   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
          4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
   0      3   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF
          2   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
          1   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
          0   C5 70 FD 21  69 08 04 00  62 63 64 65  66 67 68 69
```

Fig. 9. RFID Tag Data Block

This RFID Tag ID data transmission process is not equipped with DES cryptography security. By using another computer connected to the network, the author tries to do Sniffing using wireshark software. Results Sniffing data packets performed can be seen in Figure 10.

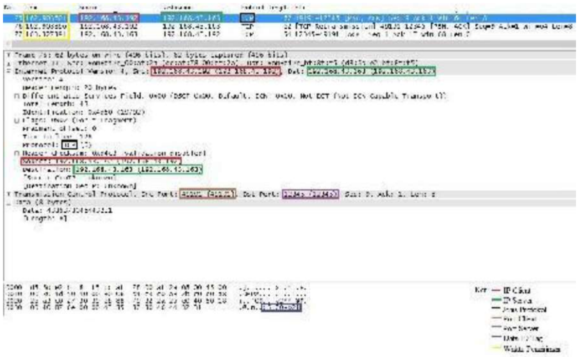


Fig. 10. Sniffing Results Without Using DES Cryptography Security

Based on the test results of sending RFID Tag ID data in Figure 4.3 it can be seen in the blue box that the Tag ID sent can be seen clearly on the side of the computer that does the Sniffing so that it can be misused by others who have no right to know.

The encrypted RFID tag ID sending test aims to determine whether the built system has been running in alignment with the original destination. To find out if the Tag ID sent has been encrypted. The author uses the sniffing scheme. Where the sniffer computer will tap the data sent from the client to the server. Capture sniffing results will be analyzed so that it can be used as a reference data to be processed. Here is a picture of capture data transmission of RFID Tag ID.

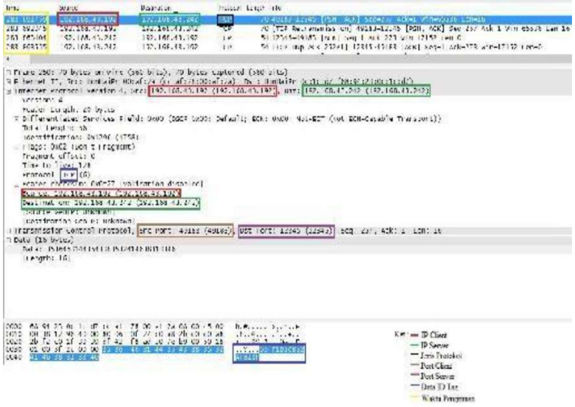


Fig. 11. Sniffing Results Using DES Cryptography Security

Based on Figure 11 which is the result of capture data transmission RFID Tag ID obtained data different from the original data RFID Tag ID. So the RFID Tag ID sent has been changed to a different RFID Tag ID. This proves that the RFID Tag ID that was sent has been encrypted.

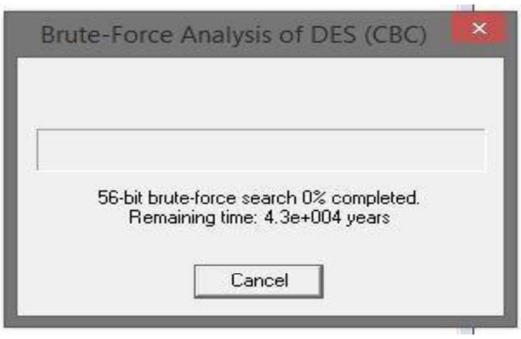
Below is the data generated in the encrypted IDID tag ID sending test.

Table 1. RFID Tag ID Encrypted Experiment

ID TAG	Kata Sandi	Kunci	Percobaan Ke 1	Percobaan Ke 2	Percobaan Ke 3	Percobaan Ke 4	Percobaan Ke 5	Data Valid
			Output ID	Output ID	Output ID	Output ID	Output ID	
20E4 BF80	1234 5678	12345678 90123456	D333A8B1 855856C2	D333A8B1 855856C2	D333A8B1 855856C2	D333A8B1 855856C2	D333A8B1 855856C2	YA
C570 FD21	1234 5678	12345678 90123456	1E3A50B7 B0329A56	1E3A50B7 B0329A56	1E3A50B7 B0329A56	1E3A50B7 B0329A56	1E3A50B7 B0329A56	YA
434F 4D50	5554 4552	13345779 9BBCDFF1	56F1D5C8 52AF813F	56F1D5C8 52AF813F	56F1D5C8 52AF813F	56F1D5C8 52AF813F	56F1D5C8 52AF813F	YA

Based on Table 1 it can be proved that the RFID Tag ID generated by the program has been run in accordance with the DES Cryptography algorithm. Thus the built system has been able to process the RFID Tag ID into an encrypted RFID Tag ID.

To find out how safe the DES algorithm can secure the tag ID, the authors perform security testing DES algorithm using the tool in the form of software cpryptool version 1.4. Here the test is done by trying to decrypt the output of the IDID tag ID that has been encrypted without knowing the key of the encryption. Due to the system being built the key is not distributed through wirelees communication, but rather the key is built directly from the software side. The technique used in testing the security of encrypted RFID tag ID is by brute force technique.



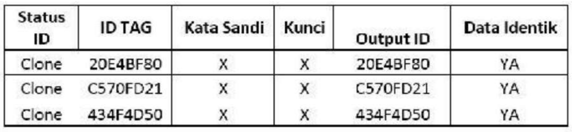
Brute-Force Analysis of DES (CBC)

56-bit brute-force search 0% completed.
Remaining time: 4.3e+004 years

Fig. 12. Brute-Force Experiment On DES Algorithm

Based on the test results that have been done, can send RFID Tag ID can be seen that the system built without the encryption is still very weak from the security side. Even in terms of wireless networks have used WPA2 PSK security password but this can still be entered with bruteforce technique. In testing experiment of RFID Tag ID security hole. The RFID Tag ID can be cloned if the RFID Tag ID value is known. Without encryption on RFID ID tags based on experimental Table 2 there are weaknesses.

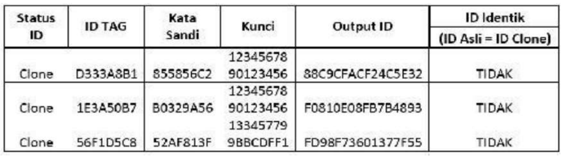
Table 2. Clone ID Tag ID Testing



Status ID	ID TAG	Kata Sandi	Kunci	Output ID	Data Identik
Clone	20E4BF80	X	X	20E4BF80	YA
Clone	C570FD21	X	X	C570FD21	YA
Clone	434F4D50	X	X	434F4D50	YA

Where ID Tags without encryption can be cloned with RFID Tag ID results that are identical to the original RFID Tag ID. This system is very dangerous if the weakness can be exploited by irresponsible party. Different if the system built there is a cryptographic security system then there will be modification of RFID Tag ID based on Table 3.

Table 3. Encrypted RFID Cloned ID ID Experiment



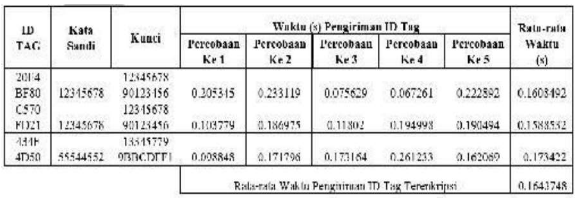
Status ID	ID TAG	Kata Sandi	Kunci	Output ID	ID Identik
					(ID Asli = ID Clone)
Clone	D333A8B1	855856C2	12345678 90123456	88C9CFACF24C5E32	TIDAK
Clone	1E3A50B7	B0329A56	12345678 90123456	F0810E08FB7B4893	TIDAK
Clone	56F1D5C8	52AF813F	13345779 9BBCDFF1	FD98F73601377F55	TIDAK

Assuming the value of the encryption result as Tag ID and keywords then the result of the cloned RFID Tag ID is not identical to the original RFID Tag ID.

In terms of encryption key is difficult to know because the key distribution is not dilakuakan in data transmission. The encryption key itself is formed from the software side so the key will not be obtained in the data transmission. For the DES algorithm encryption key there are 64 key bits. To obtain the key itself takes about 4 years with bruteforce technique based on the experiment Figure 12.

In terms of sending the encrypted RFID Tag ID (16 bit) it can still be said realtime because the delivery interval is between 0.06 - 0.26 seconds with the average time required in the delivery of only 0.164 seconds, based on experiment Table 4.

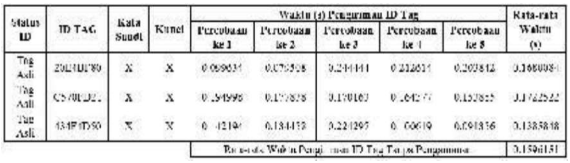
Table 4. Send Time ID RFID Tag Encrypted



ID TAG	Kata Sandi	Kunci	Waktu (s) Pengiriman ID Tag					Rata-rata Waktu (s)
			Percobaan Ke 1	Percobaan Ke 2	Percobaan Ke 3	Percobaan Ke 4	Percobaan Ke 5	
20E4 BF80	12345678	12345678 90123456	0.205345	0.233119	0.075629	0.067261	0.222892	0.1608492
C570 FD21	12345678	12345678 90123456	0.103779	0.186975	0.11802	0.194998	0.190494	0.1588532
434F 4D50	55544552	13345779 9BBCDFF1	0.098848	0.171796	0.173164	0.261233	0.162069	0.173422
			Rata-rata Waktu Pengiriman ID Tag Terenkripsi					0.1643748

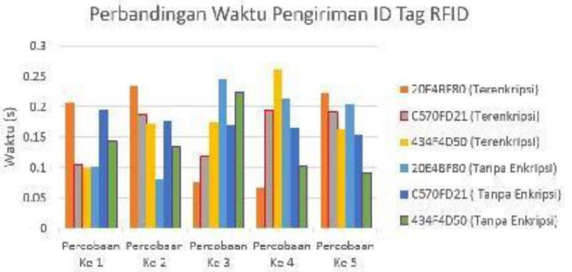
Not much different than the RFID ID without the encryption (8 bits) average delivery time of 0.159 seconds, based on the results of the experiment Table 5.

Table 5. Waktu Pengiriman ID Tag Tanpa Pengamanan



Status ID	ID TAG	Kata Sandi	Kunci	Waktu (s) Pengiriman ID Tag					Rata-rata Waktu (s)
				Percobaan ke 1	Percobaan ke 2	Percobaan ke 3	Percobaan ke 4	Percobaan ke 5	
Tag Asli	20E4BF80	X	X	0.099631	0.079508	0.244441	0.212611	0.203812	0.1680084
Tag Asli	C570FD21	X	X	0.194998	0.177878	0.170163	0.164277	0.153825	0.1722522
Tag Asli	434F4D50	X	X	0.142194	0.134413	0.221297	0.100619	0.091836	0.1385818
				Rata-rata Waktu Pengiriman ID Tag Tanpa Pengamanan					0.1596151

The second time difference is only 0.006 seconds. Here's the comparison of time comparison of RFID Tag ID without encryption and encrypted RFID Tag ID.



Based on the testing of the validity of RFID ID ID ID data without encryption in the comparison between the RFID Tag ID sector block with the output value generated then the RFID Tag ID data is declared valid. In testing data IDID IDID encrypted ID dilakuakan 2 trials data validation techniques that is mathematical and software assistance. The output value of the encryption result is compared with the encrypted value of both mathematical and software techniques. Based on test results in encrypted RFID tag IDs are valid values with actual DES algorithm results.

V. CONCLUSION

From the results of the analysis done on this final project, the writer can draw the conclusion that the Data Encryption Standard Algorithm (DES) can be used to secure the RFID tag ID that is worth 8 bits by adding user password as much as 8 bits. So 16 bit data can be encrypted with DES algorithm. A comparison of the required delivery times in 2 different systems does not present a significant difference in the delivery of RFID ID Tags without encryption with encrypted RFID Tag ID, both systems are Realtime.

In the absence of encryption process when sending RFID Tag ID will give problem to security side. Where if the RFID Tag ID data is known by the tapper then the RFID Tag ID can be cloned or faked. With DES encryption on RFID Tag ID it takes about 4 years to know the original RFID Tag ID.

REFERENCES

[1] A. Kumar, "Automatic critical health care service system using wireless communication, positioning and/or RF ID," *Proc. 2012 3rd Int. Conf. Comput. Commun. Technol. ICCCT 2012*, pp. 160–165, 2012.

[2] H. L. Shieh, S. F. Lin, and W. S. Chang, "RFID medicine management system," *Proc. - Int. Conf. Mach. Learn. Cybern.*, vol. 5, pp. 1890– 1894, 2012.

[3] L. Liu, Z. Chen, D. Yan, Y. Lu, and H. Wang, "RFID in Supply Chain Management," *Int. Conf. E-bus. E-Government*, pp. 3279–3282, 2010.

[4] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, 2016.

[5] K. Bu, X. Liu, and B. Xiao, "Fast cloned-tag identification protocols for large-scale RFID systems," *IEEE Int. Work. Qual. Serv. IWQoS*, 2012.

[6] K. Bu, X. Liu, J. Luo, B. Xiao, S. Member, and G. Wei, "Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems," vol. 8, no. 3, pp. 429–439, 2013.

[7] Kusnadi, "Pemrograman Socket," pp. 1–19.

[8] D. Rohila and N. Jain, "RFID Network Administration and Control," 2014.

[9] D. T. Rajanbabu, "Implementing a reliable cryptography based security tool for communication networks," pp. 0–3, 2014.

[10] R. Munir, *Data Encryption Standard (DES)*. 2004.

[11] H. U. I. Yue-chao and W. Yi-ming, "Secure RFID System Based on Lightweight Block Cipher Algorithm of Optimized S-Box," no. June, pp. 17–19, 2010.

[12] H. Jo and H. Lee, "A RFID Transmission System with a Security Agent," vol. 2, pp. 110–114, 2008.

[13] A. LLC, "RFID Quick Start Guide : Arduino," 2016.

[14] "Arduino Playground - MFRC522," 2017. [Online]. Available: http://playground.arduino.cc/Learning/MFRC522.

ACKNOWLEDGMENT

The authors would like to thank Mr. Reza Firsandaya Malik for his advice. This work was supported in part by the Research Laboratory of Computer and Communication Systems in Faculty of Computer Science University of Sriwijaya Indralaya, Indonesia.