Baggage Tracing and Passenger Management System in Airport Based on NFC Using Homomorphic Cryptography

Noor Cholis Basjaruddin[1], Saufik Ramadhan[2], Moch Bilal Zaenal Asyikin [3,*]
Yuni Indrianty [4], Kuspriyanto[5]

[1, 2, 3, 4]*Departement of Electrical Engineering, Politeknik Negeri Bandung, Bandung, Indonesia*
[5]*School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia*
[*]*Corresponding author. E-mail: bilalmoch@gmail.com*

ABSTRACT
Data security is one of the factors which evaluating airport service quality, starting with passenger verification and baggage management. QR Code technology security that is widely applied at this time is still considered lacking because of its characteristic that must be seen by the reader so that data can easily be copy through a camera or other image capture device. In this case, Radio Frequency Identification technology (RFID) can be applied because of its characteristic that does not require line of sight so that the data becomes safer. One of the developments of RFID technology is Near Field Communication (NFC) that enables data to be exchanged with a distance of no more than 10 cm so that in practice it very difficult to copy data between the sender and receiver because the range is too close. But, even with the right device, the data is can easily be copied, then the data encryption methods need to be added so that even though the third party succeeds in getting the data, the data can not be read. This research aimed to create a passenger and baggage management system in the airport using NFC technology. The encryption method used to secure passenger data is homomorphic cryptography. This method can simplify the encryption process and the addition of encrypted data. As the results of the testing, this system can secure data transactions because the communication distance is very close with the amount is 2 cm, then the type of tag that can be used is Mifare with 14443A standard. Finally, this system can be used to secure short-distance transactions that require the supervision of its users.

***Keywords**: Airport, QR Code, RFID, NFC, Homomorphic Cryptography.*

1. INTRODUCTION

Increasing air transportation users can create passenger-packed flow at airports, resulting in long queues at airport terminals that will indirectly affect the quality of passenger services. Airport services which are oriented towards the service users are considered very important; one of them is baggage handling.

Radio Frequency Identification (RFIF) is one of the technologies used in the aviation service sector. In 1999 British Airways implemented this technology to identify baggage, replacing barcode technology [1]. Seeing the opportunity for the increasing use of RFID in 2005, the International Air Transport Association (IATA) published the recommended practice document RP1740C [2] that contain the standards for the application of RFID tags technology as a baggage identification tool. They think this technology can increase the level of baggage management security by monitoring the movement of baggage at the airport. But, the difficulty of reaching an international agreement means this technology is not yet widely applicable.

The use of NFC technology has begun to be utilized in the aviation service industry. Air France tested NFC as a boarding-pass tool and other processes that involved authenticating passenger identities [3]. Suparta proposed the adoption of NFC technology to enhance ticketing systems with mobile platforms at airports for more efficient ticketing, gating, and aircraft boarding. But, that work does not discuss security issues or baggage tracing [4]. Ashwini Singh et al. in their research develop a baggage tracking and handling system using RFID technology and the Internet of Things [5]. Renardi et al. utilize NFC as a tool to speed up the baggage claim process at airports [6]. Pozzebon integrates a boarding pass system, indoor localization, and an information system at the airport to improve passenger services through a mobile application [7].

Even though NFC technology is wireless technology, its range is very close, which makes tapping much harder than other wireless technologies. But it still allows the data to be copied by third parties. Therefore, it is necessary to add a cryptography encryption method, which will not allow an attacker to access plaintext data on NFC tags.

As done by Diaz et al. in 2017, which developed an NFC-based baggage control system that is supported by homomorphic cryptography as one of the security features in their research [8], the use of encryption will make the system more secure.

From all the above research, it appears that the system uses NFC technology which lacks attention to data security when operating on services at airports. Therefore, in this research, the author focuses on the security system in using NFC that expected to improve the quality of service in aviation services.

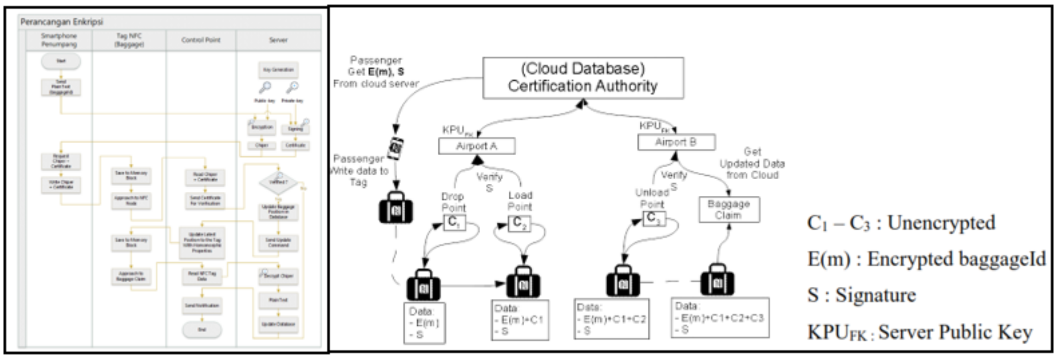
1.1. Objective

The objectives to be achieved in this research activity are:

1. Design a passenger management and baggage tracing system using NFC technology;
2. Designing an encryption system to secure data on NFC tags to be used on baggage;

2. BACKGROUND

The purpose of homomorphic encryption is to allow computation on encrypted data. Thus data can remain confidential while it is processed, enabling useful tasks to be accomplished with data residing in untrusted environments. In a world of distributed computation and heterogeneous networking, this is a hugely valuable capability [9]. The method used in the encryption design is the paillier cryptosystem, **Figure 1** shows the design for the use of the paillier cryptosystem for key generation and encryption and decryption processes which are only carried out on the server-side.



(a) (b)

Figure 1. (a) Encryption design (b) **i**llustration of homomorphic cryptography

2.1. Key-Generation

Choose any two prime numbers (p and q) whatever satisfies the following equation.

$$gcd\ (pq,(p-1)(q-1))=1 \quad (1)$$

Calculate n and λ with the following equation.

$$n=pq \quad (2)$$

$$\lambda = lcm(p-1,q-1)$$
(3)

Choose any number, where g is.

$$g \in Z_{n^2}^* \quad (4)$$

Calculate μ with the equation.

$$\mu=\left(L\left(g^{\lambda} mod n^2\right)\right)^{-1} mod\ n \quad (5)$$

$$L(u)=\frac{u-1}{n} \quad (6)$$

2.2. Encryption

To encrypt the message$M_i \in Z_n$, choose randomly $r \in Z_n^*$ and calculate chipertext as follow:

$$C_i = g^{M_i}.r^n mod n^2 \quad (7)$$

2.3. Description

To decrypt chipertext $C_i \in Z_{n^2}^*$ calculate plaintext as follow:

$$M_i = L\left(C_i^{\lambda} mod n^2\right).\mu mod n \quad (8)$$

2.4. Digital Signature

To sign message $M_i \in Z_n$, calculate digital signature (t_1, t_2)

$$t_1 = L \qquad (9)$$

$$t_2 = (H(M_i).g^{-t_1})^{n^{-1} mod \lambda} \qquad (10)$$

To verify the signature (t_1, t_2) on the message m, make sure that

$$\mathrm{H}(M_i) = g^{t_1}.t_2^n\, mod n^2 \qquad (11)$$

2.5. Homomorphic Properties

The results of the two decrypted ciphertext produce the sum between the two plain-texts.

$$\mathrm{D}(E(m_1, r_1).E(m_2, r_2)\ mod n^2) = m_1 + m_2\ mod\ n \qquad (12)$$

$$\mathrm{D}(E(m_1, r_1).g^{m_2}\ mod n^2) = m_1 + m_2 mod\ n \qquad (13)$$

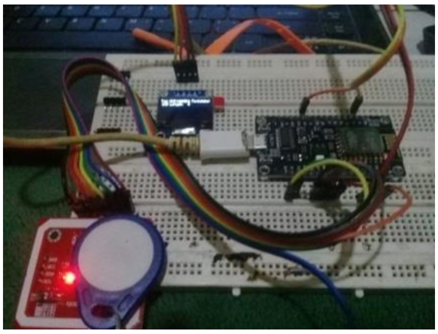
$$\mathrm{D}(E(M).(g^P.r^n)\ mod n^2) = (M+P)\ mod\ n \qquad (14)$$

3. RESULTS

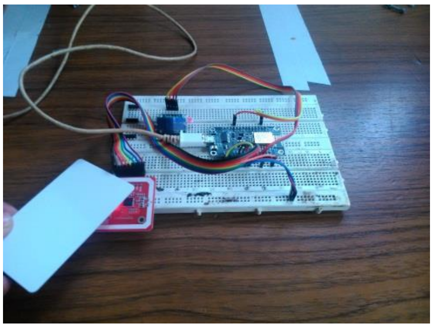
Below are the results of designing a passenger and baggage management system at the airport. This section is divided into the realization of electronics, Human Machine Interface (HMI), and the realization of display applications for passengers and encryption and decryption test.

3.1. Electronics

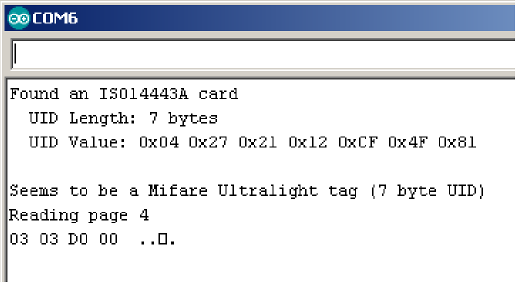
The first step is to test the NFC tag to make sure the NFC can be used for the Baggage tracing system. This test used NFC tag mifare classic and mifare ultralight and for the reader is used NFC reader module.



(a)



(b)



```
Found an ISO14443A card
  UID Length: 7 bytes
  UID Value: 0x04 0x27 0x21 0x12 0xCF 0x4F 0x81

Seems to be a Mifare Ultralight tag (7 byte UID)
Reading page 4
03 03 D0 00  ..Ð.
```

(c)

Figure 2. Testing the reading of (a) mifare classic (b) mifare ultralight (c) display response

Based on the results it can be seen that the NFC module can read tags by displaying the Identifier (UID) tag of each tag, as well as the contents of each tag in the reading block section which can be seen in **Figure 2**. In addition, reading distance testing is also done between NFC tag and NFC reader, NFC tag and smartphone, and NFC reader – smartphone (P2P). The results of testing can be seen in **Tables 1, 2, and 3** below. The test result shows that the tag reading process using either a smartphone or NFC reader must be very close to 1 cm. while the peer to peer reading process of NFC can be done up to 2 cm. the difference in reading distance may be affected based on communication mode on the NFC. Passive communication mode such as happens with NFC tags will certainly have a shorter reading distance than active communication mode as happens between NFC readers and smartphones. According to the PN532 datasheet, this distance depends on the antenna range used for the PN532 and the NFC tags antenna. From this test, the very close NFC detection distance provides security for highly confidential data transactions such as passenger account data, ticket data, and so on.

Table 1. Test results of the detection distance of the smartphone to the NFC tag

No.	Distance (cm)	Detection Status
1	10	No
2	9	No
3	8	No
4	7	No
5	6	No
6	5	No
7	4	No
8	3	No
9	2	No
10	1	Yes

Table 2. Test results for NFC tag detection distances to NFC Reader

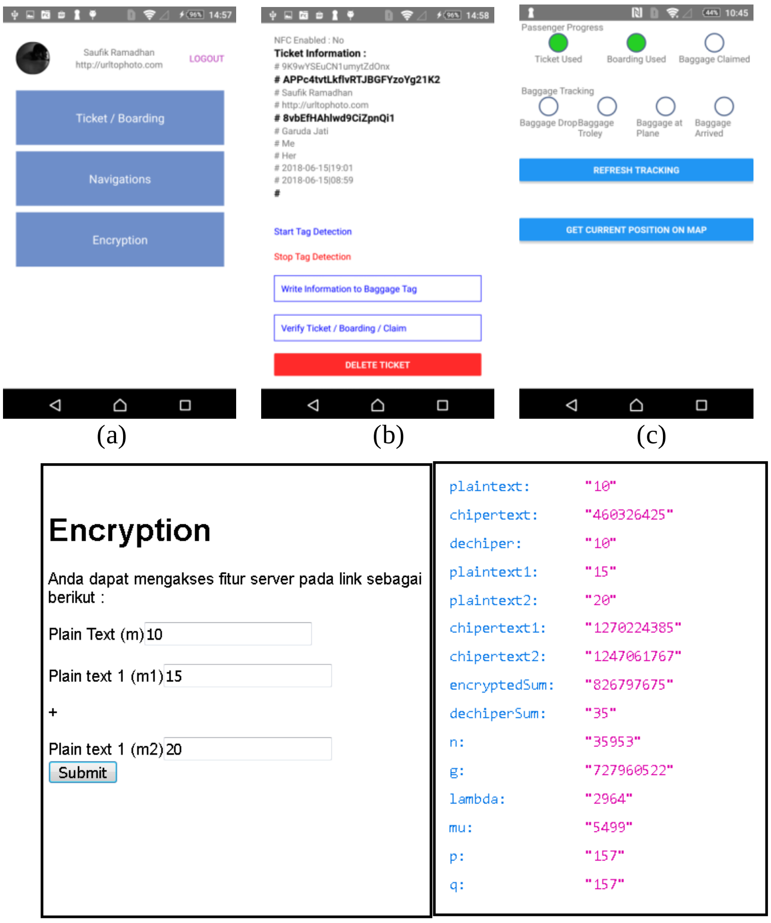
No.	Distance (cm)	Detection Status
1	10	No
2	9	No
3	8	No
4	7	No
5	6	No
6	5	No
7	4	No
8	3	No
9	2	No
10	1	Yes

Table 3. Test results of Smartphone communication distance to NFC tag

No.	Distance (cm)	Detection Status
1	10	No
2	9	No
3	8	No
4	7	No
5	6	No
6	5	No
7	4	No
8	3	No
9	2	Yes
10	1	Yes

3.1. Human Machine Interface (HMI)

The HMI system is made in the form of a mobile application-based HMI system that functions to display the status of passengers and baggage. Also as a medium of data exchange between passengers and the airport.



(a)

NFC Enabled : No
Ticket Information :
9K9wYSEuCN1umytZdOnx
# APPc4tvtLkflvRTJBGFYzoYg21K2
Saufik Ramadhan
http://urltophoto.com
# 8vbEfHAhlwd9CiZpnQi1
Garuda Jati
Me
Her
2018-06-15|19:01
2018-06-15|08:59
#

Start Tag Detection
Stop Tag Detection
Write Information to Baggage Tag
Verify Ticket / Boarding / Claim
DELETE TICKET

(b)

(c)

Encryption

Anda dapat mengakses fitur server pada link sebagai berikut :

Plain Text (m) 10

Plain text 1 (m1) 15

+

Plain text 1 (m2) 20

Submit

```
plaintext:      "10"
chipertext:     "460326425"
dechiper:       "10"
plaintext1:     "15"
plaintext2:     "20"
chipertext1:    "1270224385"
chipertext2:    "1247061767"
encryptedSum:   "826797675"
dechiperSum:    "35"
n:              "35953"
g:              "727960522"
lambda:         "2964"
mu:             "5499"
p:              "157"
q:              "157"
```

(d) (e)

Figure 3. (a) Main page, (b) Ticket page, (c) Navigation page, (d), (e) Testing Paillier Cryptosystem

3.2. *Encryption and Decryption*

Encryption and decryption algorithm testing aims to compare the results of the calculation of encryption and decryption of data using the Paillier cryptosystem with the Paillier cryptosystem program that has been made. The result of the test in Figure 3 (d), (e) shows that the data sent from plaintext is successfully encrypted.

3.3. *Overall Testing*

The overall testing is done by using the system from the beginning user's registers as a passenger, through the application, until baggage claims. The overall test results on the system can be seen in Table 4. The test function that is successfully done using the system created is such as registration, login, booking, ticketing, tracking, and baggage claims.

Table 4. Overall function testing

No.	Command	Worked	failed	Output
1	User Account Registration	✓		User Accounts in Database
2	User Account Login	✓		Display the Main Page of the Application
3	Book a flight ticket	✓		Display ticket information on the ticket page
4	Write Ticket Information to the NFC tag	✓		Ticket data is read on the NFC tag
5	Drop baggage at the drop point (NFC Reader module)	✓		Drop points respond by displaying baggage that has been detected, the Navigation Page in the application shows that baggage has arrived at the drop point
6	Boarding Pass	✓		The NFC module responds by displaying that the boarding pass was successful
7	Tracking	✓		The application displays the points that have been passed
8	Baggage Claim	✓		The NFC Claim module responds by displaying that the baggage claim was successful

4. CONCLUSION

According to the test results and to sum up this research, the conclusion is NFC baggage tracking and passenger management systems using homomorphic cryptography have been designed and successfully realized according to the expected functions and specifications. The distance reading NFC technology is suitable to be applied for close-range transactions. But on the other side, this technology is not suitable to be used in the tracking systems because it can be difficult if there is a packed-condition of baggage queues on the automatic system. The tags that can be used in this baggage tracking system are tags with Mifare type with a reading standard of 1 4443A.

5. RECOMMENDATIONS

Based on the functional realization of the system, this system can work according to the specified specifications. For further development, the author suggests using other RFID technology with further reading distances. So that it can be utilized on the systems that run automatically, and it will do not need much supervision from the officer.

ACKNOWLEDGMENT

This research was funded by DRPM Grant 2019 (Contract Number: 2/E1/KP.PTNBH/2019) from the Indonesian Ministry of Research, Technology, and Higher Education.

REFERENCE

[1] R. Boden, July 2013. [Online]. Available: https://www.nfcworld.com/2013/07/03/324876/british-airways-to-offer-nfc-luggage-tags/.

[2] "IATA Recomended Practice RP1740c," in IATA Joint Passenger Service Conference, Geneva, 2005.

[3] Future Travel Experience, Agustus 2010. [Online]. Available: https://www.futuretravelexperience.com/2010/08/nfc-enabled-mobile-phones-the-future-of-the-check-in-process/.

[4] W. Suparta, "Application of near field communication technology for mobile airline ticketing," Journal of Computer Science, vol. 8, no. 8, pp. 1235–1243, 2012.

[5] A. Singh, S. Meshram, T. Gujar and P. R. Wankhede, "Baggage Tracing and Handling System using RFID and IoT for Airports," in *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, 2016.

[6] M. B. Renardi, Kuspriyanto, N. C. Basjaruddin and A. Prafanto, "Baggage Claim in Airports using Near Field Communication," Indonesian Journal of Electrical Engineering and Computer Science, vol. 7, no. 2, pp. 442-448, Agustus 2017.

[7] A. Pozzebon, "The PITAGORA project: Near Field Communication to improve Passenger Experience in Airports," in 2017 IEEE International Conference on RFID Technology & Application (RFID-TA), Warsaw, 2017.

[8] N. Álvarez-Díaz, P. Caballero-Gil and M. Burmester, "A Luggage Control System Based on NFC and Homomorphic Cryptography," *Mobile Information Systems,* vol. 2017, no. Article ID 2095161, p. 11 pages, Februari 2017.

[9] A. Anastasios, January 20. [Online]. Available: https://www.venafi.com/blog/homomorphic-encryption-what-it-and-how-it-used/.