OPEN ACCESS
Indo-JC Indonesia Journal of Computing
ISSN 2460-9056
socj.telkomuniversity.ac.id/indojc

Ind. Journal on Computing
Vol. 4, Issue. 2, Sept 2019. pp. 55-66
doi:10.21108/indojc.2019.4.2.309

Multi-Factor Authentication Using a Smart Card and Fingerprint (Case Study: Parking Gate)

Isa Mulia Insan[1], Parman Sukarno[2], Rahmat Yasirandi[3]

School of Computing, Telkom University
Telekomunikasi Street Bandung (022) 7564108 Bandung, Indonesia

[1] muliainsan@student.telkomuniversity.ac.id
[2] psukarno@telkomuniversity.ac.id
[3] batanganhitam@telkomuniversity.ac.id

Abstract

Security is one of the considerations in the development of smart parking. In Indonesia, the most common authentication factor is using a smart card as an authentication factor at the gate. The use of smart cards as an authentication factor has loopholes that can be misused. Therefore an additional factor is needed for authentication. Authentication that uses more than one factor is also called Multi-Factor Authentication (MFA). However, MFA applied to smart parking can still be misused. The cause of the MFA can be misused is because the MFA cannot ensure the user's smart card. So, in this study applying the MFA at the gate in smart parking using a two-factor authentication system. These two factors are smart cards and biometric (fingerprint) data. This authentication system can solve problems where if the smart card is lost, the smart card can be used by other owners (P1), if the data smart card has been cloned, it can be a threat to the system (P2) and if the data is rewritten, it can become a threat to the system (P3). The ability of the system to overcome these problems is proven by passing several attack scenarios. Thus, the security of the proposed parking gate system can be guaranteed. Besides, the system has also passed a user agreement testing, in which the test results obtained by the proposed system experience an overhead time of 3.24s. However, the proposed system overhead time is still within the tolerance limit because the results of the proposed system safety comparison test have increased compared to the existing system.

Keywords: Multi-Factor Authentication, Smart parking, Smart card, Fingerprint, Biometric

Abstrak

Keamanan merupakan salah satu pertimbangan dalam pembangunan smart parking. Di Indonesia, faktor autentikasi yang paling banyak ditemui adalah menggunakan smart card sebagai faktor autentikasi pada gerbang. Penggunaan smart card saja sebagai faktor autentikasi memiliki celah yang dapat disalahgunakan. Maka dari itu dibutuhkan faktor tambahan untuk autentikasi. Autentikasi yang menggunakan lebih dari satu faktor disebut juga dengan Multi-Factor Authentication (MFA). Tetapi, MFA yang diterapkan pada smart parking masih dapat disalahgunakan. Penyebab MFA dapat disalahgunakan adalah karena MFA tersebut tidak dapat memastikan smart card user. Sehingga, pada penelitian ini menerapkan MFA pada gerbang di smart parking dengan menggunakan sistem autentikasi dua faktor. Dua faktor tersebut adalah smart card dan data biometric (fingerprint). Sistem autentikasi ini dapat mengatasi permasalahan yang mana apabila smart card hilang, smart card bisa digunakan oleh selain pemilik (P1), Apabila Smart card datanya telah cloning, dapat menjadi ancaman bagi sistem(P2) dan apabila Smart card datanya telah ditulis ulang, dapat menjadi ancaman bagi sistem(P3). Dapatnya sistem mengatasi permasalahan tersebut terbukti dengan melewati beberapa skenario serangan. Sehingga, keamanan sistem gerbang parkir yang diusulkan dapat dijamin. Selain itu sistem juga telah melewati user agreement testing, yang mana hasil pengujian yang didapat oleh sistem yang diusulkan mengalami

Received on August 2019. Accepted on Sept 2019

waktu overhead sebesar 3.24s. Walaupun demikian, waktu overhead sistem yang diusulkan masih dalam batas toleransi karena, hasil dari pengujian perbandingan keamanan proposed system telah meningkat dibanding sistem yang ada.

Kata Kunci: Multi-Factor Authentication, Smart parking, Smart card, Fingerprint, Biometric

I. Introduction

SEVERAL types of factors for authentication have been used in smart parking in Indonesia. Authentication factor generally uses a smart card as an authentication factor [1]. Smart cards as one of the authentication factors have loopholes that can be misused, which can be used by unauthorized parties when the smart card is lost or dropped. Therefore, it is proposed to use more than one authentication factor or also called Multi-Factor Authentication (MFA) to cover the lack of authentication using smart cards only.

The application of smart cards in the MFA is not new to smart parking. In research [2], [3] has implemented a smart card as one of the MFAs on smart parking. However, the smart card can still be misused. The cause of the abuse at the MFA is implemented it cannot ensure the smart card system user or user. Based on these problems, then the purpose of this research was to use the level of authentication factor others, namely biometric data that can ensure the user's smart card when authentication.

This research applies the MFA at the gate in smart parking using a two-factor authentication system. Two factor authentication is used on the system, so the system can authenticate a smart card user using biometric data. These two factors are smart cards and data biometric (fingerprint). In its application, the authentication system is divided into two levels. The first level is to check data on the smart card, and the second level is biometric data compatibility user and biometric data stored on the smart card.

II. Methodology

The method used in this research used the Design Science Research Methodology (DSRM). The use of this method is focused on problem-solving and system development. In Figure 1 shows 6 stages carried out in this research. The first step is identifying problems and motivation. The output of this stage is in the form of review literature from several studies related to smart parking. Next is the identification of the object of the solution to the problem. At this stage, the review literature is also carried out on several studies related to biometrics and MFA. Both stages are done in chapter III. The third stage is design and development. At this stage, the design and model of the system are thoroughly carried out from the analysis that has been carried out in the previous stage. The fourth stage is implementation. This stage is an implementation of the MFA that was designed in the previous stage. This phase is the making of hardware and coding software needed. The third and fourth stages are explained in chapter IV. The fifth stage is the evaluation stage in which the system is tested to answer the problem. This fifth stage described in chapter V. The final stage is the conclusion. At the conclusion (sixth stage) describes how the design results until the evaluation meet the objectives mentioned earlier. This conclusion stage is written in chapter VI.

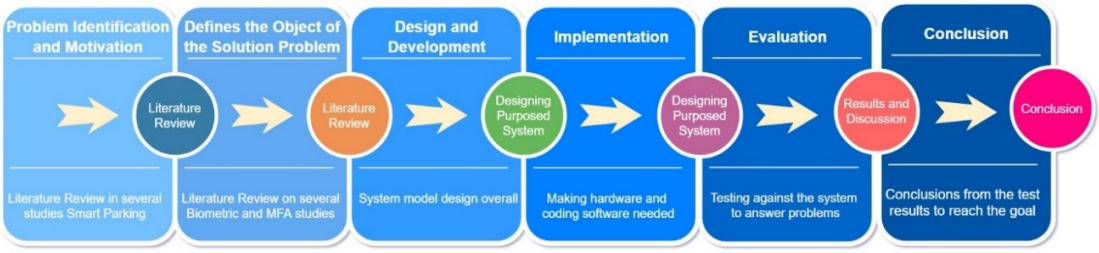

Fig. 1. Stages of Research Methodology

III. Literature Review

Security at smart parking is one of the considerations for vehicle owners. In the Table I showed a comparison of several authentication methods existing and proposed parking system.

TABLE I
Comparison of Methods for Smart Parking Authentication

Method	RFID	OCR	GSM	Biometric
A Secure Parking Reservation System Using GSM Technology [4]			√	
Smart parking Management System Using RFID and OCR [2]	√	√		
Smart parking System using RFID and GSM Technology [3]	√		√	
Proposed System	√			√

One of the authentication systems what is used in smart parking is using Global System for Mobile Communications (GSM) technology as smart parking reservations. In the use of GSM technology, the user gets a password via message. The password is used to exit and enter the parking area[4]. In the application of this technology, if a user's mobile phone changes hands, other people can easily carry out vehicle theft. Therefore, authentication has required the user (owner) of the smart card.

There are also those who use Radio frequency identification (RFID) and authentication smart parking. In the research [2] used RFID and Optical Character Recognition (OCR) to authenticate the user smart parking. In this research, the system detects RFID tags from vehicles and uses OCR to recognize vehicle number plates. Besides being combined with OCR, RFID has also combined with GSM [3]. However, the system still can be covered by theft. Smart cards that are owned by the user are smart cards that can be lost and can be misused by others. If the smart card has changed hands to someone who is not authenticated, then that person can access the smart parking easily. Aside from the smart card, the system that is applied only does authentication using objects that are owned; there is no authentication for the user.

In addition to Smart parking, MFA has also applied to several studies. Research [5] combines two factors in authentication. Two factors are used, namely the location of the user with a username and password as an authentication factor in the mobile application login. The combination of these two factors aims to make mobile application authentication safer.

The application of 3 levels has also been built in research [6]. In that research, it has combined id-password, a device (handphone), and biometric (face recognition) for authentication before being able to access the application. The purpose of using these three authentication factors is to make mobile application authentication safer in a simple way.

The proposed system applies an authentication system using smart cards and biometric data. It was explained in the research [7] that biometric technology included fingerprints, sounds, hand geometry, palms, irises, and facial recognition. Among the biometric technologies listed, a fingerprint is the most commonly used [8]. In several studies [8], [9] fingerprint has been used as an authentication factor to open the entrance. Therefore, biometric data used in the system is fingerprint data the user.

The application carried out on the system is to use Uid smart card and biometric data planted into the smart card. The authentication used is using Uid and biometric data matching that has been embedded in smart cards with biometric data from the user (real-time). So, the ongoing authentication that using smart cards is cannot be manipulated or changed hands with other people.

IV. Designing Purposed System

A. Problem Design

The proposed system will be designed to answer the following problems:

P1: If the smart card lost, the smart card can be used by other than the owner.

P2: If the data smart card has been cloned, it can be a threat to the system.

P3: If the data Smart Card has been rewritten, it can be a threat to the system.

To prove the system that can solve the above problems, then the system is tested with attack scenarios. The attack scenarios is described in chapter IV part of the testing procedure, and the test results are explained in chapter V.

B. System Design

Before the system design, it showed and explained some of the hardware used for authentication on the system. Figure 2 indicated prototype and some of the hardware used by the system.

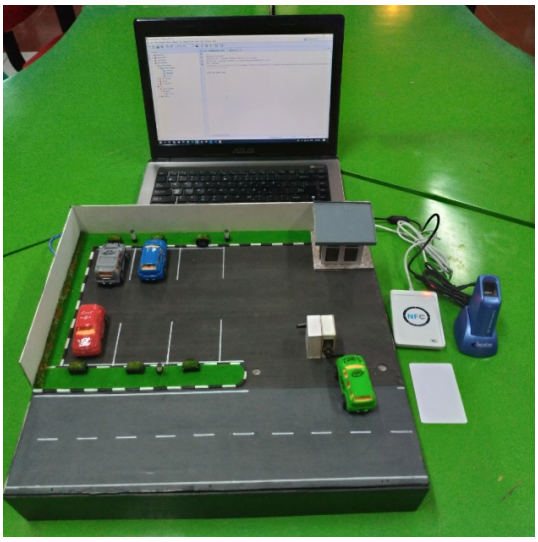

Fig. 2. The smart gate prototype uses the proposed system.

The fingerprint scanner used is Secugen Hamster Plus. The accuracy of the fingerprint scanner is known from FAR (False Accepted Rate) and FRR (False Rejected Rate) biometric. FAR is an assessment in which the user authentication is not to later regarded as the user authentication, while the FRR is where the assessment carried out by the user authentication rejected authentication. The test results carried out by NIST 's MINEX are FAR as significant as 0.06 % and FRR as big as 0.23 % [10].

Next, are smart cards and smart cards reader/writer. The smart card used is Mifare 1k. This mart card has a memory capacity of 1kilobyte. Memory on a smart card is consist of 16 sectors, where each sector has 4 blocks, and each block has 16byte of data that can be read/written. Smart card the reader/writer used to read Mifare 1k is a contactless ACR122u smart card reader/writer. ACR122u uses USB to communicate with computers. ACR122u has a led and buzzer as a marker that the card is detected. The commands used to use this tool have also been documented [11].

System design that applies Multi-Factor Authentication (MFA) shown in Figure 3 :

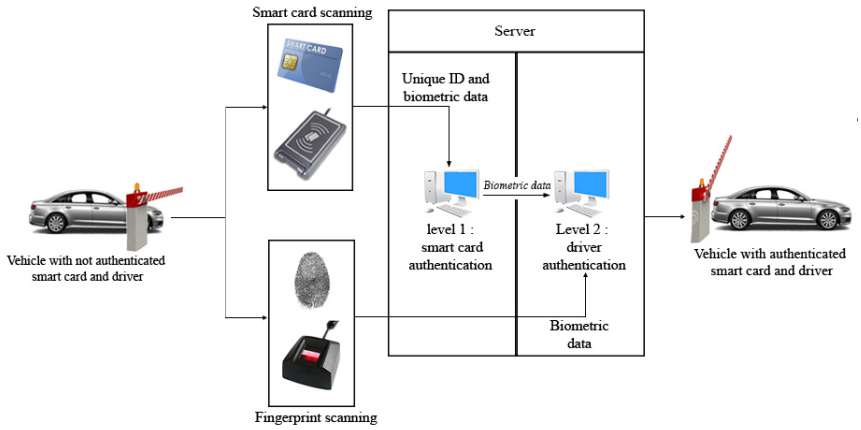

Fig. 3. System Architecture

In Figure 3 shown gates are installed at the entrance and exit of the smart parking system. At the gate, embedded a smart card reader, and also a fingerprint scanner. Users who want to access the smart parking are required to scan a smart card. Furthermore, the user must do a fingerprint scan to authenticate the user, so that only vehicles with a smart card and user authentication that the tar can get into the smart parking.

A First level authentication, the user does a smart card scan on smart card reader provided. In this scan, the smart card used must have Uid and biometric fingerprint of the user, and also both of them have been registered on the system. So, the system can authenticate a smart card to the user.

The second level, the system takes biometric data from the user in real-time from the fingerprint scanner. Then biometric data matching was carried out users are taken in real-time, with biometric data stored on the smart card before. Matching biometric data that is done aims to authenticate the user who uses a smart card. After the smart card and user authentication, the gate can be opened, and the vehicle can access the smart parking.

C. Technical Planning and Mechanism

Technical design and the mechanism of the system applied is presented in Table II. The technical planning and mechanism carried out is the need for hardware (hardware), software (information systems), and brainware (human resources).

TABLE II
PLANNING AND TECHNICAL MECHANISM

Aspect	Item	Mechanism
Hardware	- Barrier gate	- The parking lot is designed automatically, with a system that is connected with a smart parking transaction information system
	- Smart card	- Smart cards that are used must be detectable by smart cards reader and can store Uid data and biometric data (fingerprint) in byte form
	- Smart card reader	- Smart card reader used can read and write data on the smart card

Aspect	Item	Mechanism
	- Fingerprint scanner	- The scanner that is used must be able to retrieve biometric data (fingerprint) from the user.
Software	- Registration system - Authenticati on system	- This system is used for smart card registration and registration fingerprint. - This system can authenticate the smart card and the user by using Uid and biometric data obtained from the smart card reader and fingerprint scanner
Brain-ware	- Operator - User	- Operators must be able to operate the registration and maintenance system - In system implementation, users get a smart card that has been registered

D. Design System Registration

Before designing the MFA system, the stages and data exchanges were carried out when enrollment. This enrollment system is designed so that registered data can be used to authenticate smart card and user. The data registered on the system is Uid data from the smart card and biometric data from the user. First, the system takes biometric data from the user using a fingerprint scanner. After that, data biometric and Uid of the smart card is stored in the system database. Finally, the smart card and user can authenticate the system.

E. Scheme Proposed MFA

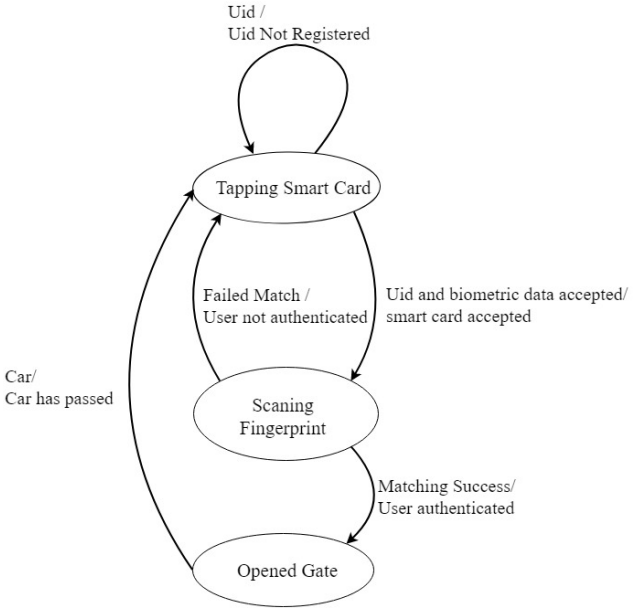

Fig. 4. Finite State Machine Diagram of Multi-Factor Authentication

In Figure 4 shown that output is based on input and state. First, the user must tap the smart card. When tapping a smart card, the system takes Uid and biometric data on the smart card. If Uid and biometric data on the smart card have registered, then the smart card is received, and the user can go to the next state. If it is not registered, the smart card is rejected, and the user must return to the initial state. Then the user performs a fingerprint scanning. Data biometric scanning results match those of biometric data which takes from the smart card. If the matching results match, then the user is proven to have been authenticated. So the gate opens, and the vehicle can pass through the gate. If it is not suitable, then the user is proven not authenticated, and the user must return to the initial state, namely tapping the smart card. After the gate opens, the user can pass through the gate, and finally, the gate closes again.

F. Proposed MFA Protocol

The proposed authentication has two levels. The first level is the authentication smart card, and the second is user authentication. This section describes the standards used in the relationship and the transfer of data between devices.

In Figure 5 shown sequence diagram MFA is used in the system. The sequence diagram has two parts, namely authentication smart card and user authentication. Authentication smart card process ran when the smart card SC is scanned into the smart card reader SCR available. The smart card has a block [n], where n is a count number (0-63) with a total of 6 4 blocks. The US authentication system authenticates Uid and data biometric stored in a smart card. The details are explained below.

1) *SCR → SC: Command APDU "auth"*

   SCR send APDU command authentication to SC. The APDU command is used to authenticate SC block before the SC block can be read.

2) *SC → SCR: 2 bytes (90 00 / 63 00)*

   SC respond to APDU Command sent by SCR. The response given is in the form of success (90 00) or failed (64 00)[11]. This response indicates whether the block can be read or not.

3) *SCR → SC: Command APDU "read block" [n=0] and [4-37! = (n mod 4 = 3)]*

   SCR send the APDU command to read the block on the smart card. All blocks read are blocks where Uid and biometric data saved.

4) *SC → SCR: Uid and Biometric data (fingerprint)*

   SC send data APDU response block of Uid and biometric data. The response sent is a Uid byte and biometric data planted in SC.

5) *SC → AS: Uid and Biometric data (fingerprint)*

   Uid and Biometric data which is obtained from the smart card reader, sent to the authentication system AS. Uid is used to be authenticated by the system. And then if Uid is registered, biometric data forwarded for the second level of authentication process.

After authentication smart card process is done, the next step is authentication on the user or the owner of smart card. Authentication used is biometric data from user fingerprint obtained from Fingerprint scanner FS with biometric data taken from the smart card. Authentication explanation biometric is as follows:

1) *FS → F: Detect F*

   The FS detects the fingerprint of the user. This detection is used to obtain biometric data from the user.

2) *F → FS: Data Biometric*

Users scan F on the provided FS. This step is used to obtain biometric data from user.

3) *FS → AS: Data biometric*

Biometric data of user, matched with biometric data obtained from smart card at the previous level. This matching is done to authenticate smart card from the user.

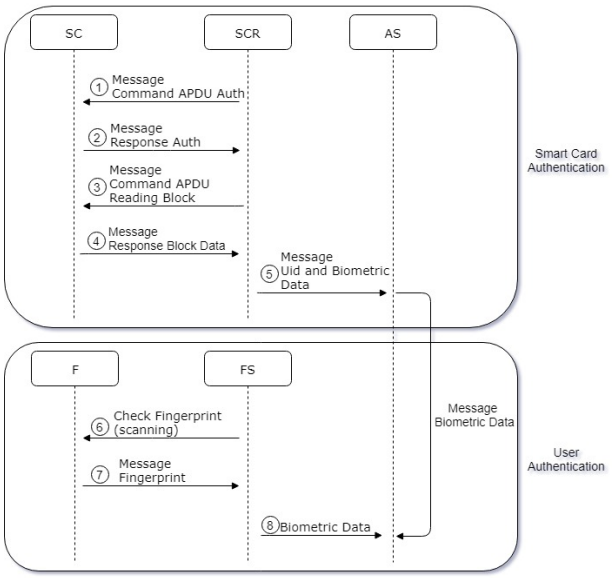

Fig. 5. MFA Protocol Sequential Diagram

G. Testing Procedure

Before testing, the pre-conditions of the testing scenario must be determined:

1) *The system must have an open gate when authentication is successful.*

2) *The system has a smart card as one of the authentication factors.*

In the testing phase, two testing procedures are carried out on the existing system and the proposed system. First is the system security comparison testing procedure, and the second is the system overhead testing procedure. System testing procedures Comparison of systems used for testing can be seen in Table III.

TABLE III
System Comparison

System	RFID	Biometric
Existing system	√	
The proposed system	√	√

1) *System security testing:* The first system testing procedure is carried out to obtain a safety comparison of the proposed system with the existing system. Besides, the tests carried out also aim to prove that the system can overcome the problems mentioned earlier. The existing system uses authentication factors in the form of RFID, while the proposed system uses authentication factors in the way of RFID and biometric data. To get a security comparison of the two systems, several attacks are used that can occur in the smart parking authentication system. Some of the attacks and scenarios that can arise in smart parking authentication are as follows:

a. *An attacker uses an authenticated smart card to enter the smart parking:* The attacker passed the authentication system with an authenticated smart card. Next, the system authenticates to the smart card. However, the smart card that held with attackers are not the ones who pitch authentication. So that the expected result is the authentication fails, and attackers cannot enter. The results of this test are used to prove whether P1 can be overcome. The testing scheme is shown in Figure 6.

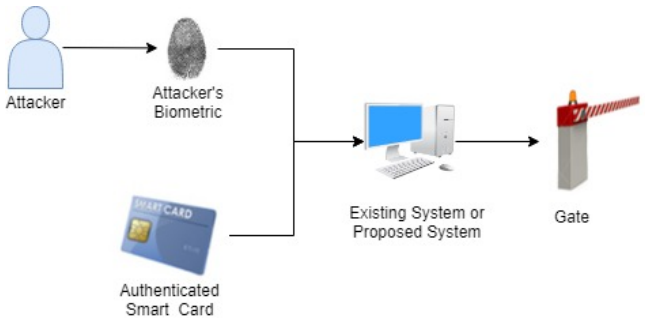

Fig. 6. Scheme of Scenario Testing 1

b. *An attacker uses a smart card clone from the authenticated smart card:* Attackers passed the authentication system using a smart card clone. Systems authenticate the smart card clone that is used. So, the expected result is that system authentication fails, and the attacker cannot enter. The results of this test are used to prove whether P2 can be overcome. The testing scheme is shown in Figure 7.

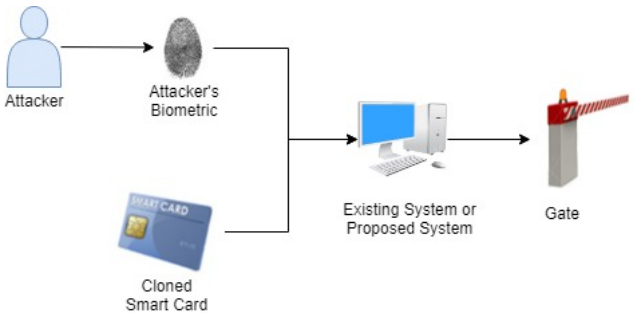

Fig. 7. Scheme of Scenario Testing 2

c. *The attacker uses an authenticated smart card whose data is changed using attacker data:* The attacker passes an authentication system with a smart card whose data is changed using attacker data. The system authenticates the smart card used. So, the expected result is that system authentication fails, and the attacker cannot enter smart parking. The results of this test are used to prove whether problem three can be overcome. The testing scheme can be seen in Figure 8.

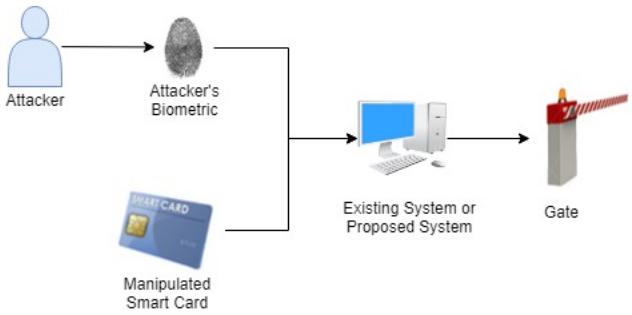

Fig. 8. Scheme of Scenario Testing 3

2) *User Agreement testing:* The second testing procedure, is user agreement testing. The purpose of this testing is to find out changes to the system performance proposed to answer the problems mentioned earlier and get opinions from users about the proposed authentication system. The performance changes to be tested are the length of time needed for authentication until the gate opens. This test is carried out on ten people, where each person authenticates ten times. Total test carried out is 100 times on each system. After testing each system, the user is asked a question. The question that is given to the user is "whether the transaction time of the proposed system is still within the tolerance limit or not". That question can prove whether the proposed system is feasible to be used instead of the existing system.

V. Results and Discussion

In this section the test results are presented using the two procedures described in the previous section.

A. System Security Testing

The test results using the first procedure can be seen in Table IV. The results obtained from testing using the first scenario is that the attacker can pass the existing authentication system and enter the smart parking. It can happen because the system only authenticates using Uid smart card that cannot ensure the user of the smart card. The existing system failed to authenticate in testing the first scenario. Next is the result of testing the first scenario using the proposed system. The results obtained are that the attacker cannot pass the authentication system. Because at the second level authentication, the system cannot take authenticated biometric data. The system can ensure that the user is not an authenticated person. Therefore, the proposed system has successfully authenticated on testing the first scenario. This result also proves that the proposed system can overcome the problem P1. The original owner can only use smart cards on the proposed system.

The test results using the second scenario are as follows. On existing systems, the attacker can bypass authentication using a smart card cloning. It is possible for an attacker to pass the authentication system because the system only authenticates a smart card using Uid. When the attacker has another smart card data that have cloned with Uid of an authenticated smart card, then the system of the attacker passed the authentication system. So that the existing system failed to authenticate in testing the second scenario, for the results of testing the second scenario using the proposed system, the attacker cannot pass the authentication system because the system can ensure the user on the smart card authentication second level. Thus, the proposed system managed to authenticate in testing the second scenario. Besides that, it also proves that that the proposed system can overcome the problem P2. Smart cards from cloning cannot be a threat to the proposed system.

The results of the third scenario testing on the existing system are that the attacker can enter using a smart card whose data has been replaced with attacker data. Because on the existing system it only authenticates the UID of the card. As a result of the test results on the proposed system are that the attacker cannot pass the authentication system using a smart card with the biometric data has been changed using the attacker's biometric data. It is impossible for an attacker to pass through the authentication system because, at the first level, the system authenticates data stored on the smart card. So, when a difference is found in the data, the

system knows, and authentication fails. Therefore, testing the third scenario in the proposed system is successful. This result also proves that the proposed system can overcome the problem P3. Smart cards whose data is changed, cannot be a threat to the proposed system.

TABLE IV
RESULT OF TESTING

Scenario	The Existing Authentication Parking System	The Purposed Authentication Parking System
Scenario 1	The attacker succeed to penetrate the system	The attacker failed to penetrate the system
Scenario 2	The attacker succeed to penetrate the system	The attacker failed to penetrate the system
Scenario 3	- The attacker succeed to penetrate the system	The attacker failed to penetrate the system

After testing, the proposed system can overcome the two problems mentioned. In addition to answering the problem, testing carried out also proves that the system can ensure smart card users. So, the proposed system can avoid misuse of smart cards by unauthenticated people.

B. User Agreement Testing

The test results using the second procedure can be seen in Figure 9. The test results obtained are that the existing authentication system gets an average time of 3.88s whereas the proposed system receives an average authentication time of 7.12s. The time difference obtained from the two systems is 3.24s. From the results of testing the second procedure it can be concluded that by adding an authentication factor to the system, it will cause an increase in the time of the system transaction. So that the proposed system experiences overhead but, from the results of the questionnaire survey it was found that the overhead time that arises in the proposed system is still within tolerance because the results of the proposed system security testing have increased compared to the existing system.

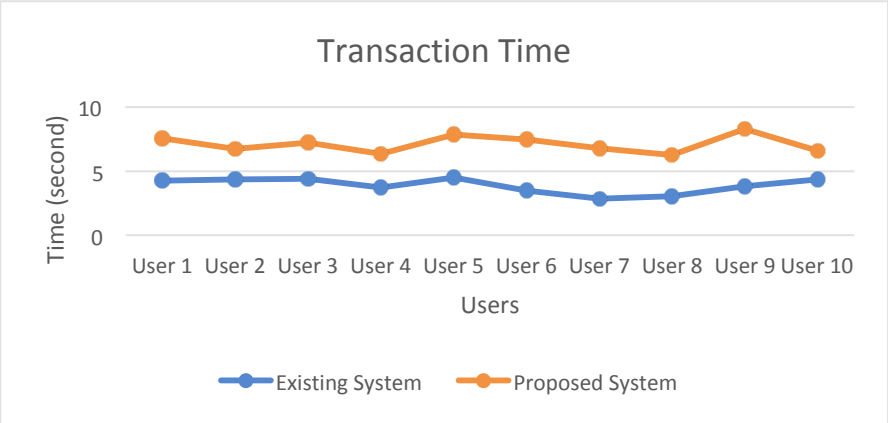

Fig. 9. the test results using the second procedure

VI. CONCLUSION

This authentication system can be guaranteed security because the system can overcome several attacks from the test scenario. From the results of the tests carried out, the smart card can only be used by people who have the right to use it, so the proposed system can reduce the concern of users who lose smart cards and identity theft. Besides, the transaction time needed by the system is still within the tolerance limit so that the proposed system can replace the existing system.

In the future, this authentication system can be applied to systems that implement smart cards as one of the authentication factors. Such as attendance, and security at the door. Also, the system can also use the e-ID card which is owned by every citizen and also stores data as a fingerprint smart card.

Acknowledgement

Thanks to the Internet of Things Studio and the Forensic and Security Laboratory, Telkom University, Indonesia, which have been the sites for this research. As a wish, this research can make a significant contribution to the development of technologies in the world.

References

[1] Y. A. Setyoko and R. Yasirandi, "Security Protection Profile on Smart Card System Using ISO 15408 Case Study : Indonesia Health Insurance Agency," *2018 6th International Conference on Information and Communication Technology (ICoICT)*, pp. 425–428, 2018.

[2] Y. Joshi, P. Gharate, C. Ahire, N. Alai, and S. Sonavane, "Smart parking management system using RFID and OCR," *International Conference on Energy Systems and Applications, ICESA 2015*, pp. 729–734, 2016.

[3] L. Kumar, M. H. Khan, and M. S. Umar, "Smart parking system using RFID and GSM technology," *IMPACT 2017 - International Conference on Multimedia, Signal Processing and Communication Technologies*, pp. 180–184, 2018.

[4] Y. Rahayu and F. N. Mustapa, "A Secure Parking Reservation System Using GSM Technology," *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, pp. 518–520, 2013.

[5] K. I. Ramatsakane and W. S. Leung, "Pick location security: Seamless integrated multi-factor authentication," *2017 IST-Africa Week Conference, IST-Africa 2017*, pp. 1–10, 2017.

[6] A. Bissada and A. Olmsted, "Mobile Multi-Factor Authentication," *The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017)*, pp. 210–211, 2017.

[7] R. Devi and P. Sujatha, "A study on biometric and multi-modal biometric system modules, applications, techniques and challenges," *2017 Conference on Emerging Devices and Smart Systems, ICEDSS 2017*, pp. 267–271, 2017.

[8] A. Siswanto, K. R. Ku-Mahamud, and N. Katuk, "Biometric Fingerprint Architecture for Home Security System," *Innovation and Analytics Conference & Exhibition (IACE)*, vol. 3, pp. 137–141, 2016.

[9] J. Baidya, T. Saha, R. Moyashir, and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*, 2017.

[10] P. Grother *et al.*, "MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template," *National Institute of Standards and Technology*, 2006.

[11] Advanced Card Systems Ltd, *ACR122U USB NFC Reader Application Programming Interface*, V2.04. Hongkong, 2018.