Jurnal Ilmiah KURSOR
Menuju Solusi Teknologi Informasi

Vol. 10, No. 2, Desember 2019

ISSN 0216 – 0544
e-ISSN 2301– 6914

ANALISYS AND IMPLEMENTATION CLOUD-BASED BIOMETRIC AUTHENTICATION IN MOBILE PLATFORM

[a]Agostinho Marques Ximenes, [b,1]Sritrusta Sukaridhoto, [c]Amang Sudarsono, [d]Hasan Basri

[a,b,c,d]Informatic and Computer Department
Electronic Engineering Polytechnic Institute of Surabaya, Surabaya, Indonesia
E-mail: [a]Agusmarques1@gmail.com, [b]dhoto@pens.ac.id

Abstract

Based on the Indonesian Central of Statistics the level of poverty people in September 2018 was 25.95 million, based on data, the government allocation care fund the reduce poverty people, the fund is given through the bank. However, banks cannot allocate funds because the cost for build infrastructure is expensive, such as making an ATM. about that, the banks need to find a new solution to allocation care fund to the poverty people, Mobile Platform Biometric Cloud Authentication is one solution. In this study, the experimentations of the biometric face recognized (face data encrypt and decrypt by algorithm AES 256 bit) to secure online payment mobile application based on the QR Code scan and face recognition. The concentration of this study lies in the experiment of biometric face recognition and QR Code scan on biometric payment based face recognition and QR Code scan mobile applications that play a role in data communication security. The test results on this mobile application show that scanning a QR Code and biometric face recognize can be implemented at an online merchant transaction with an accuracy of 95% and takes 53, 21 seconds in transactions.

Key words: Biometric, Cloud server, Cryptography, QR Code.

[1] Corresponding Author

INTRODUCTION

Based on the Indonesian Central of Statistics the level of poverty people in September 2018 was 25.95 million, based on data, the government allocation care fund the reduce poverty people, the fund are given through the bank. However, banks cannot allocation funds because the cost for build infrastructure is expensive, such as making an ATM [1].

Technology developments and human dependence on technology, and as well as technology have penetrated in various fields, such as industry, manufacturing, education, government, business, banking, and daily human life [2].Mobile as one of the services that are very developed nowadays, because with mobile it is very helpful and makes it easy for users to be able to access data and information anywhere without being limited by media, space, time to access the data and information desired and faster and cheaper. But the security side as one of the obstacles is often faced in the form of data theft, data interception, fraud, and unauthorized data access [3,14].

The system used in security today consists of a data security system using cryptography and biometrics and QR Code [3]. Cryptography is a technique hidden original text to random text using keys. Biometric uses human characteristics in the form of fingerprints, retinas, faces, palms, DNA, and soles of the feet to authenticate [4].

The security technique of data transactions using cryptography still has weaknesses such as interception, manipulation, theft, destruction, and data manipulation. so also using biometric techniques such as duplicate characteristics of human body parts that are used as security keys.

From these problems which will be discussed as follows: (1) Providing solutions to disburse public funds by building mobile transaction applications, (2) Disguising biometric data so that biometric data is not easily faked. (3) Performing a combination of QR Code, biometric (face) and cryptographic (AES 256 bit) systems in order to produce a stronger, reliable and safe authentication level, (4) Accuracy at the level of biometric authentication for transactions, and (5) Measuring how long the time needed to make a transaction.

The various problems that have been identified, this researchers propose a new solution give to the bank for allocation care fund to the poverty people is Mobile Platform Biometric Cloud Authentication is one solution..

Biometric face recognize

Biometrics is a technique for identifying someone by using the characteristics of one part of the human body [5]. One part of the human body used in this research is biometric face recognize. A person's recognition technique uses face recognizes is security system for lock the door or mobile face lock [4,6].

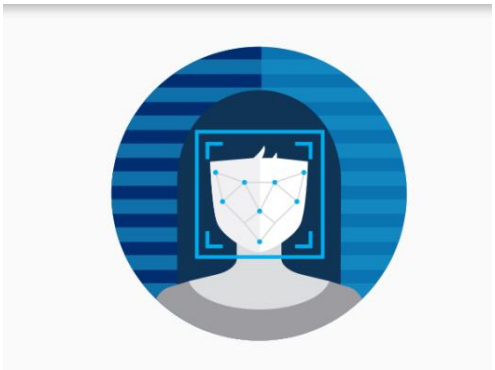


Fig 1. Face recognize biometric

Figure 1 explains that a person's face data can be saved, changing it into a character and send into the database. Recognition of facial patterns with making a rectangle on the face to determine the face pattern and position to take the value [5,13,14]. Authentication using face recognition has two main processes, (1) the process of identifying faces by performing facial positioning, (2) determining attributes are taken to conduct training to detect faces and faces recognition processes by matching faces between face data that have intersected in the database with taking a new face photo [4,14,15].

Android Mobile APPS for Digital Payment

Android Mobile apps are applications made for smartphones, can be installed and operated on the Android smartphone platform. Android mobile apps run on Java programming. Digital payment is a digital-based transaction concept. in Figure 2.

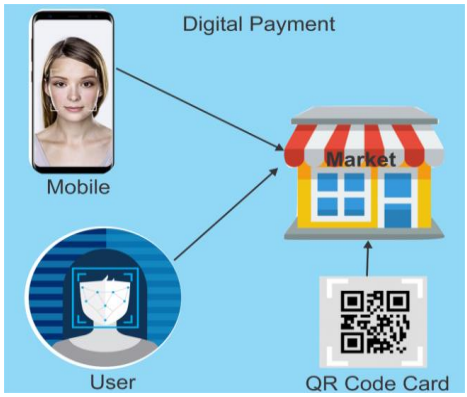


Fig 2. APPS Android Mobile for digital payment

In figure 2, there have three design system and literature support research about, 1 (QR Code, (2) merchants, and (3) biometric face recognize.

1. QR Code

QR Code (Quick Response Code) is two dimensions that can store data. A QR code is used for the first time in the automotive world to track parts of a vehicle. The growing use of QR Code is widely used to spread website addresses. Contact numbers, email addresses, telephone numbers, even for payments. So the presence of a payment system that is currently and which will continue to develop technology, using a payment system with one payment system technology QR Code (Quick Response Code) or QR Payment as a solution to address human needs for safe and efficient transaction data security. Illustration of the QR Code in figure 3 [10].

Fig 3. QR Code [10].

2. Face Application Programming Interface (API) Azure

Azure Face API is a cognitive service algorithm for detection, recognition, and analysis of human faces in images. Cognitive algorithms can process information that has a human face, and that information can be implemented into a variety of IU/ UNIX security systems on mobile and robots[5]. The Azure cognitive service is a cloud-based service and develops artificial intelligence [5,10]. In the Face API, there are two processes, (1) face detection API to detect human faces in images and make square location coordinates on faces. After the face has been extracted, the features extraction related to facial attributes such as poses, head poses, gender, age, emotions, facial hair, and glasses as in Figure 4. (2) Face verification API to authenticate with taking new face data with mobile camera and then send to the face API for detection and matching face data in the database as in fig 5 [5,13,14,6].

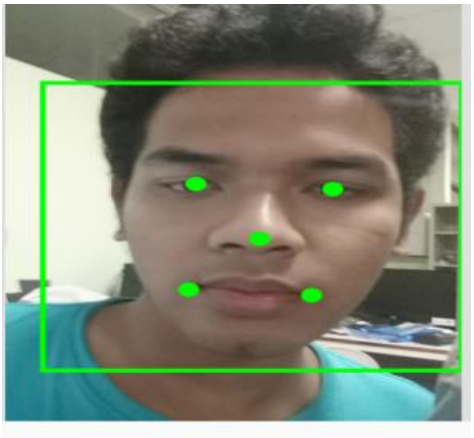


Fig 4. Face detection

In figure 4 are the face detection process and the right side of image 5 as a face verification process.

Fig 5. Face detection

3. Merchant

Merchants are sellers of goods or services that have a business form (physical store) or

online store that collaborates with the Bank in providing services for receiving payments via e-money of the bank concerned [9]. Merchants are divided into two is individual merchants and legal merchants. Individual merchants are individual merchants without being based on the procedures and provisions for establishing legal entities, whereas authorized merchants are merchants established based on the procedures and regulations for the establishment of applicable legal entities. After an individual or business entity registers as a merchant, then they will obtain a merchant ID [9] — illustration of merchant in figure 6.

Fig 6. Online merchants system [9]

3. Mobile Cloud Computing

Mobile cloud computing is one of the infrastructures of stores data and processes they are carried out outside of mobile devices [7,8], mobile devices move computing and store data not directly on mobile devices but data storage in the cloud. A very important feature of the mobile cloud platform is collaboration functionality between the mobile platform and the cloud, and access via wireless based on the web-based or client on the mobile platform [12,16,17,18].

This section of the paper has four purposes: Section 1 presents the background of the problem in this paper, the related works and a previous study of the research presents in section 2. Section 3 presents the details of the system was built, Section 4 presents the results and discussion of the system of our research. Section 5 present future work that will be conducted for the extensions of our project research.

RELATED WORKS

Xiaoxue Wang, Yufan Zhang and Huichen [23], with the title Cloud-based mobile system for biometrics authentication (IEEE) research, results in Handwritten Cloud-based Internet services. While this study has differences in authentication using face recognizes. The equation in this research is the cloud base data store.

Soyuj Kumar Sahoo and S R Mahadeva Prasanna [10], with the research title Bimodal Biometric Person Authentication Using Speech and Face Under Degraded Condition (IEEE) with the results of the Biometrics System research using facial and voice features (speech and Face Features). This research is similar to face authentication without using cryptography, while this study uses face data encryption using 256 AES cryptography and uses QR Code.

Philip Tresadern, Timothy F. Cootes and Norman Poh [12], with the research title Mobile Biometrics: Combined Faces and Voice Verification for a Mobile Platform (IEEE) with Sytem security results and personal verification on mobile with a combination of real-time face and sound (face and voice verification). This research has similarities in the use of mobile and face recognition, while the research conducted by researchers lies in the Cloud base and face encryption and decryption.

Omri, F, Foufou, S, Hamila, R and Jarraya, M [24] with the title of a cloud-based mobile system for biometric authentication (ITS Telecom) research results on authenticating cloud computing technology with signatures. In this study the differences in authentication, this study uses handwriting while the research conducted by researchers using face recognition.

Xudong Cao, Yichen Wei, Fang Wen, Jian Sun [25] in the title Face Alignment by Explicit Shape Regression (Int J Comput Vis) the results of research using explicit forms of regression are combined with correlation to produce highly accurate results to determine facial position from grammar (landmark face data set). This study is divided into the experimentationn of face recognition, in this case, only the face detection is done, as little as the research carried out does face recognition and is used to authenticate transactions.

Ahmad Amran, Surya Michrandi Nasution, Fairuz Azmi [9] with the title Experimentationn of Cryptography Algorithm For Biometric Payment (e-proceeding of

engineering) results of the research by securing biometric payment systems based on fingerprint authentication. Vol.3, No.1 April 2016. This research equation is located in 256-bit AES cryptography, merchant payment, while this research uses authentication fingerprints while research conducted by researchers using Face Recognize.

In the research conducted by researchers using a QR Code as a personal identification card, face data is encrypted and decrypted with 256 bit AES algorithm cryptography and used as transaction authentication, and the system implemented for merchant payment online transaction authentication. The application runs on the Android mobile device and also the cloud server store database.

SYSTEM DESIGN

Mobile Platform Biometric Cloud architecture

Mobile Platform Biometric Cloud Authentication architecture is a mobile platform transaction authentication using 2 authentication methods with a scan QR Code and faces verification permissions and biometric data based on the cloud server. This biometric authentication application is implemented to authenticate merchant transactions by banks and users. In this application, there are two main process stages in running the application which consists. Illustration in figure 7.

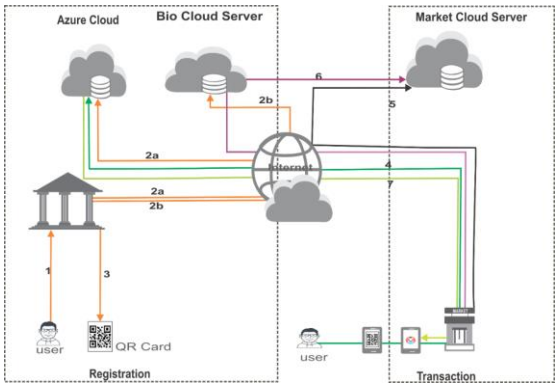


Fig 7. Mobile Platform Biometric authentication architecture

The process details of the mobile biometric cloud authentication architecture platform in Figure 7, has 2 step architecture process;

A. Registration process

1. The user goes to the bank (1)
2. Enrlment data personal and take picture face user and then sento the face API Azure database for training dace detection user(2a), with SSL.
3. After face detects, the face data sebto to a cloud server (2b), with SSL.
4. Create QR Code user cards from face user data in the database (3).

B. The Transaction Process

1. The user goes to the shopping merchant store and goes to the cashier and payment (5), scans the QR Code card(4).
2. Check the balance, check the user balance permissions at the bank with the amount of goods to be paid (6).
3. Perform permission transactions with face detection or recognize (7).

Design system mobile platform biometric cloud authentication

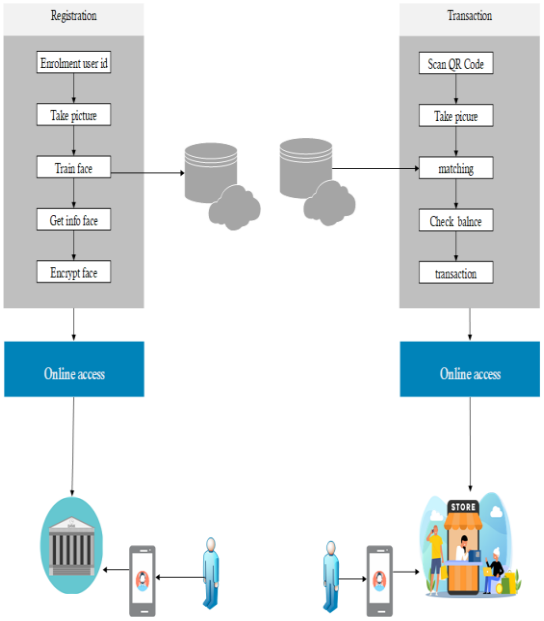


Fig 8. Design of Mobile Biometric Cloud Authentication Platform system

Design of the system that has been 2 processes, (1) registration process, (a) enrolment data user, (b) takes photos sending to the Azure face API, (c) training face to detect face on picture, (d) after training getting information from training face data, (e) face encrypted, (f) after encryption Face data sent to the bio database cloud server. (2) Transaction process, (a) scans the QR Code user,(b) takes photos new face on image, (c) matching and detection face on pictures on the

bio database cloud server, and before matching the-data in decryption, (d) checking balance on bank and amount for paid, data communication lines with SSL . Illustration in figure 8.

Face detection and recognize flow on Face API Azure

1. Face detection flow

Face detection is the process of performing human face detection in an image using the azure face API, illustration flow in figure 9.

In figure 9 is the flow for face detection on the photo, there are 5 flows for face detection, namely (1) starting, (2) inputting data and taking face photos, (3) resizing the face with 200X200 PX size, (4) face send data SSL to Azure Face database training and face detection in the image, (5) data face save.

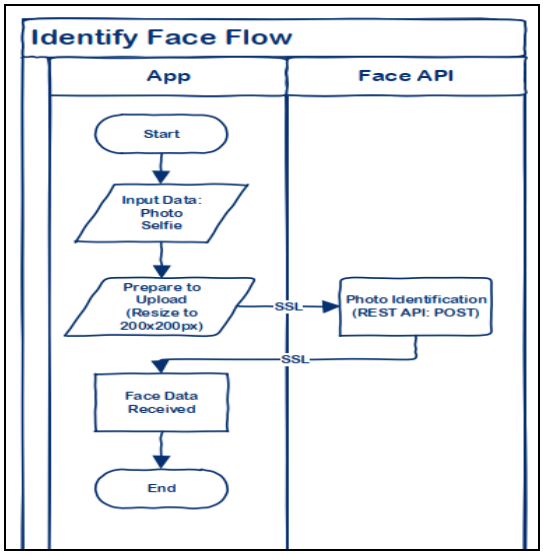


Fig 9. Face Identification Flow

2. Face recognize flow

Face recognize is a detection and face verification or recognize user. Illustration in figure 10.

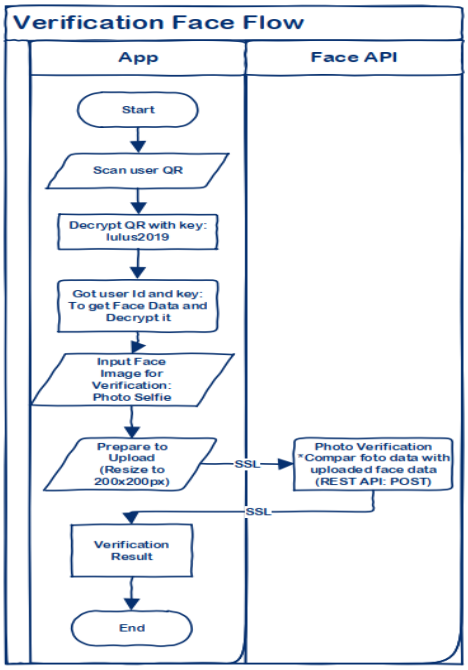


Fig 10. Face verification flow

In figure 10 is recognize face flow there are 9 flow, namely (1) start, (2) scan QR Code, (3) decrypt QR Code, (4) get user id and key decrypt face data, (5) take photo face, (6) doing photo resizing with a size of 2000X200 px, (7) sending photos to the face database API training face detection, and doing face comparisons or face matching, (8) verification results, (9) completed.

Mobile platform Biometric Cloud Authentication Flow

Mobile platform biometric cloud authentication flow is the registration and transaction flow.

1. Enrolment user

User enrollment flow is a process for registering user data and user face IDs. Illustration in figure 10.

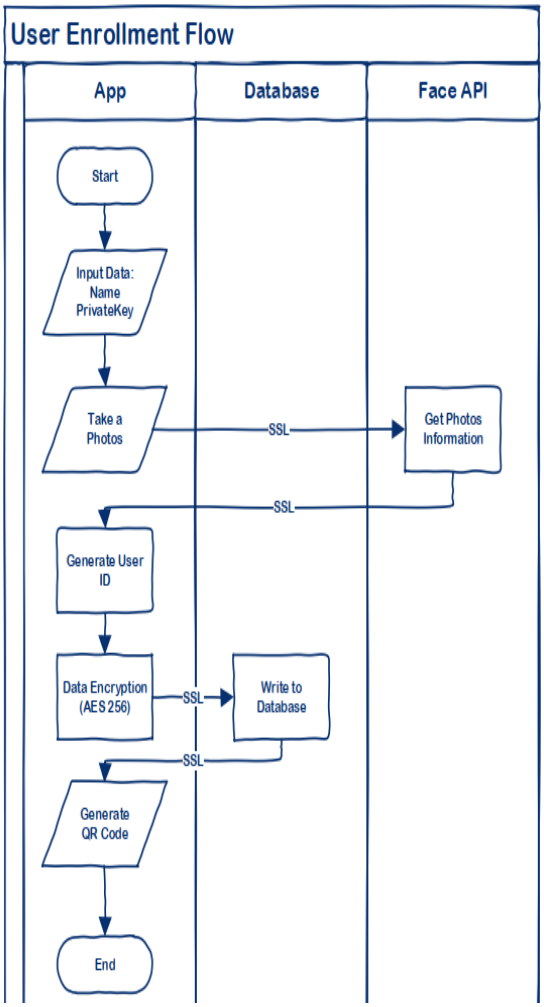


Fig 11. User enrolment flow

In Figure 11 is the flow for registering user and face biometric data, in the initial stage of inputting user data and inputting AES key, taking the face image in the picture and sending it to the face API database via SSL to perform face detect and encrypt face ID, send user and face data to the biometric cloud server database, creates a QR Code person card and finishes it.

2. Verification flow

User verification flow is the stage for transaction permissions use scanning the QR Code and face verification. Illustration in picture 12.

In figure 12 is a flow scan QR code and face verification, there are 9 flow, namely (1) start, (2) scan QR Code, (3) read QR code and decrypt, (4) obtain data face from database, (5) perform face decryption, (6) take face photos, (8) send SSL to Azure face API to detect Face and face comparison, (9) perform face verification or face matching and finish.

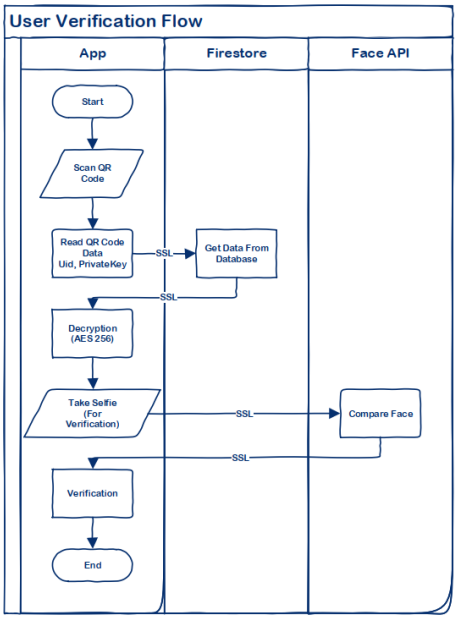


Fig 12. Transaction flow

3. Transaction flow

Transaction flow is a process for making transaction permissions. Illustration of transaction flow in Figure 12.

In figure 13 is the user transaction flow, the flow is as follows; (1) verification process, (2) if verification is input amout to pay, (3) if verification is not successful show transaction result , (4) if balance amount pay transaction enough transaction enable, (5) parse transaction result, (6) show transacton result and end.

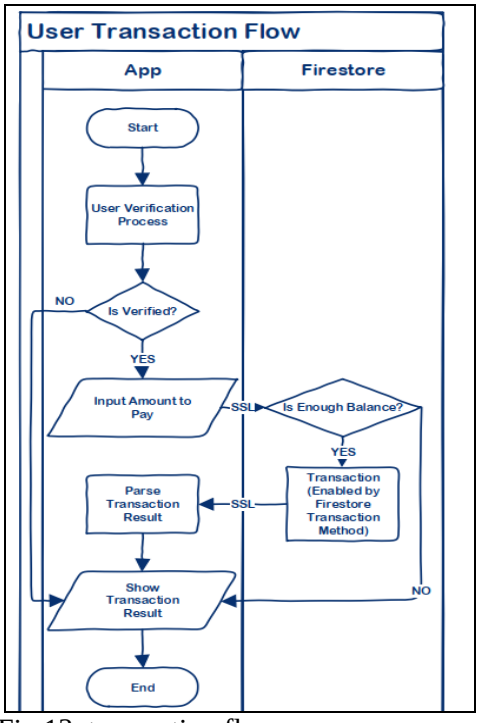


Fig 13. transaction flow

Mobile Biometric Cloud Authentication Platform Menu

1. Main Menu

The UI / Unix menu is used for the main menu of the authentication cloud biometric application, illustrated in figure 14.

Fig 14. Main menu

In Figure 13 as the main UI.UNIX there are three menu processes; User registration process menu as a menu for user id and face id data registration, transaction process menu to scan QR code face recognize and payment, and as well as a guide menu as an instruction to use mobile biometric cloud authentication apps.

2. Registration Menu

The registration menu is UI / UNIX to register user data. Illustration in figure 15.

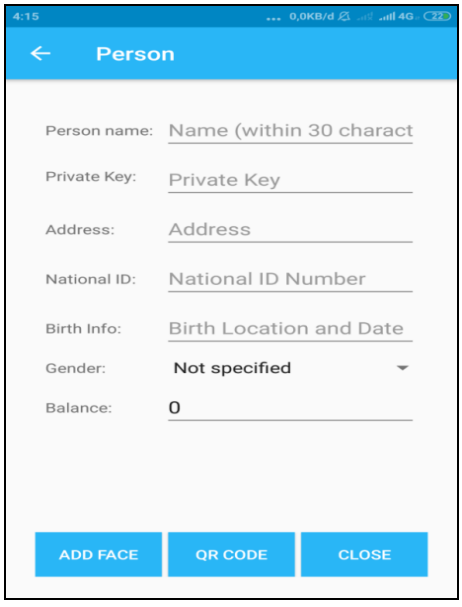


Fig 15. Registration menu

The registration menu in Figure 15 as UI for Registering there are 7 columns, there are columns (1) person names for inputting user names, (2) private keys as keys for encrypting face people, (3) addresses as input addresses, (4) national ID for inputting KTP number, (5) birth info as input for place and date of birth, (6) gender as sex person (7) balance as input balance amount in the bank. And there are 3 action buttons, namely (1) the add face button for the action of taking the face, (2) the QR Code to create the QR Code user, and (3) the close button to exit the registration menu.

3. QR Code Scan for transaction Menu

Scan menu is a process to scan QR Code users.. Illustration 16.

In figure 16 it is a scan of the QR Code by using the rear camera on the mobile by directing the QR Code card to the camera and inputting the amount of money to be paid into the input number of transactions using the Rupiah.

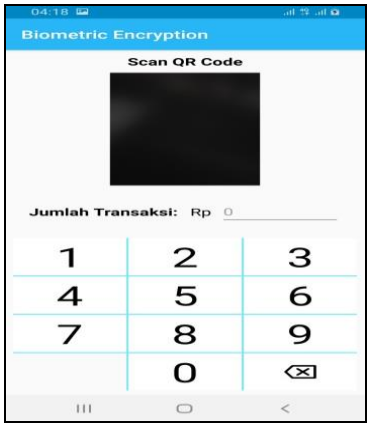


Fig 16. Scan QR Code menu

4. Verification for transaction menu

In the process of performing transaction permissions. in illustration 17.

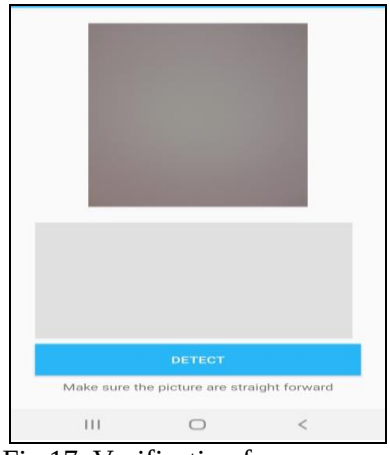


Fig 17. Verification face menu

In figure 17 is a process menu for face verification in the image, there are 2 parts, (1) the box at the top is the place to take a new photo face, (2) the buttom box to display the face detected by using a new face. While on the detect button to perform face detection on the database.

RESULT AND DISCUSSION

In this results sections, we have done some experiment and present the experimentationn both of software and hardware development. The experiment has been given the results that performed as well and using the analytical test showed how the system that we built works well. Several test registration and transaction permission for merchant transactions.

A. Registration experimental

In the registration menu process, there are 3 main processes, namely;

1. The enrolment user id and face id experimental

Registration of the process menu consists of 4 processes, namely, (1) user-id input, (2) taking face images, (3) face detection, and (4) process for storing databases. The illustration is in table 1.

In the table 1 enrollment process, part number (1) of the user-id process menu has several attributes used, namely, (a) name txt area input the name user, (b) private key as input to lock key face person images using 256-bit AES algorithm, (c) address for inputting user address, (d) national-id as input for KTP number, (e) birth info input place and date of birth, (f) gender for sex user, and (f) balance payment at the bank.

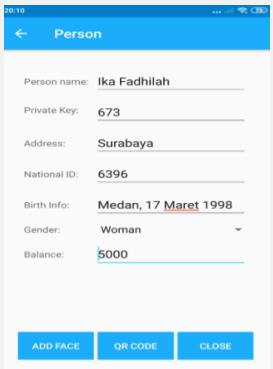
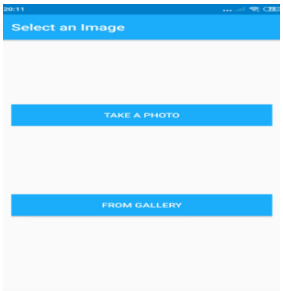
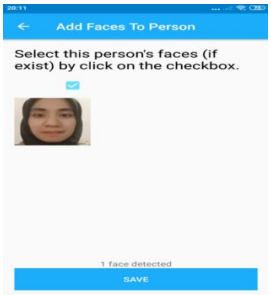
In the process of enrolling table 1. part number (2) has 2 processes, namely (a) input face with the take button a photo is used to take face photos in real-time or directly with the back camera and (b) with a button from gallery used to input images face from.

In the process of enrolling table 1, part number (3) is the process of taking a face photo with a back camera in real-time or directly.

In the process of enrolling table 1, part number (4) is the result of the face detection process in the photo taken.

In the process of enrolling table 1, part number (5) is a face person data in the database bio in cloud server.

Table 1. Registration menu experimental

No	Procedure	Image
1	**Input user-id**	
2	**Take Picture**	
3	**Face detection**	
4	**Save face-id**	
5	**View biometric face on data base**	

2. Store data face to the cloud server

Storage data face is dabase for store user id and face id. Fig 18.

In the experimentationn of the bio store database in the cloud server in Figure 18. The database built using MongoDB. Database bio, having column 12, (1) the id object is clean id face, (2) person-faces contain the number of photos stored in the database, (3) the name includes the name of the user, (4) the person-id id of the person, (5) the private key contains 256-bit AES algorithm key for face encryption. (6) URL is the URL of the network, (7) balance is the user balance in the bank, (8) gender contains the gender of the user, (9) address as the residence address of the user, (10) nid is the id ID of user, (11) TTL is the place of birth date, and (12) V is the sum of the faces.Create QR Code experimental.

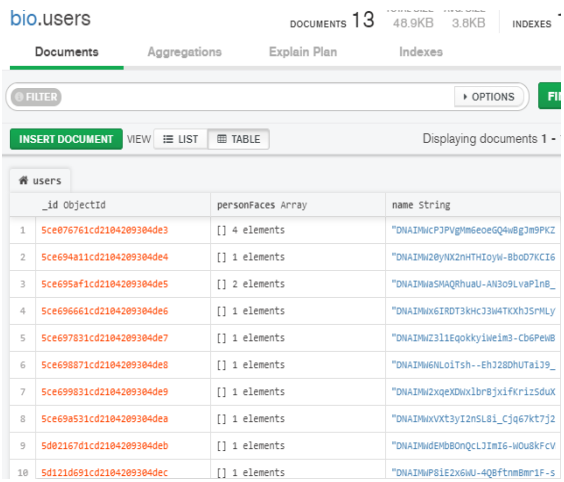


Fig 18. Store data cloud server

3. Create QR Code

This is implemntation of creating a QR Code for user identication card. Illustration of the user QR Code in figure 19.

Fig 19. Create QR Code

In the experimentationn of creating a QR Code user card fig 19. Using the face id user on the database and dame encrypt face to create QR Code user.

B. Transaction permission experimental

In the implemntation of transaction menu , there are 7 processes, namely (1) scan the QR Code, (2) face detection, (3) face verification, (4) store transaction data, (5) input amount to pay (check balance), and (6) transaction permissions.

1. Test Menu Process Scan QR Code

Experimentationn of the scan menu process QR Code. in Figure 20.

Fig 20. QR Code Scan

The results of the experimentationn scan the QR Code in fig 20, scan QR Code there are two stages, namely, (1) input the amount of money will be paid into the text are, (2) showing the QR Code card to the camera back of the mobile and scan. And the scan process will continue to the next process.

2. Face-detection-and-verification experimental

(1)take a picture (2) face detection

Fig 21. Face detection experimental

The results of the experimentationn face detection process in fig 21. Face detection process 2 step, namely (1) taking photos with the front camera and showing on rectangle photo area and (2) pressing the detect button to decrypt the face user and matching faces if there are any face data user in the database it provides detect results like in the right side of fig 22.

3. Verification face experimental

In this process, it is a step to verify face and transaction. Test on illustration 22.

Fig 22. Verification face experimental

In the face verification process experimental in Fig 12. it is the permission transaction process, there are two steps, namely (1) after the face has been detected and press verifies button to verification face, (2) after the verification process to do permission transactions for check balance paid, if balance showing transaction success.

4. Store market cloud sever experimentally

Storage transaction data is a process for storing market transaction data in the cloud server market database. Illustration of transaction data storage test in figure 23.

In the trial store data transaction test on the market database in the cloud server with the SSL network cloud server address, image 23 with the name of the market database, table transaction and there are 7 columns consisting of (1) id face data content object, (2) transaction-id contains transaction data, (3) user-id is id of user, (4) merchant contains transaction place data, (5) balance before contains user balance before deducted by transaction, (6) transaction amount contains the total transaction, (7) balance after containing the balance in the bank.

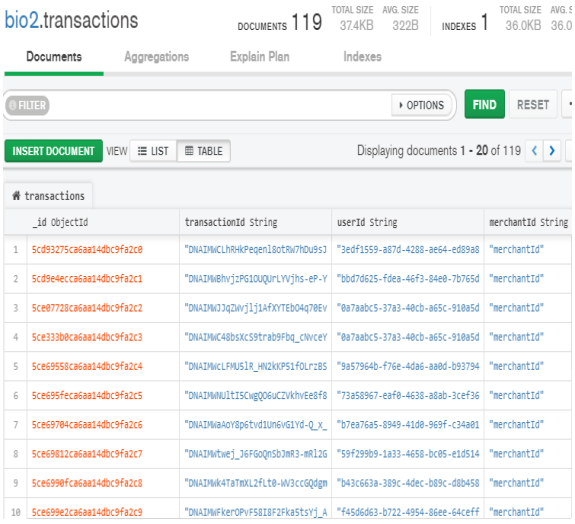


Fig 23. Store market cloud server

5. Check balance experimental

At this stage, perform transaction balance check, an illustration of transaction in fig. 24

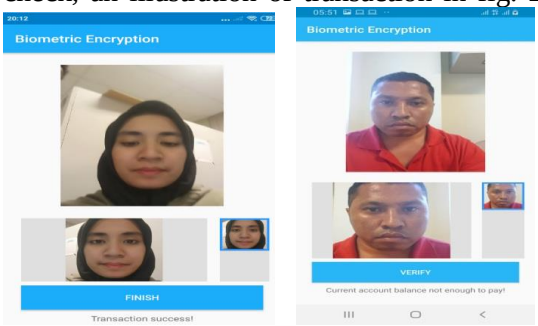


Fig 24. Check balance

In figure 24 is a trial of a balance transaction, in testing the balance of Transaction using two conditions, namely, condition (1) transaction success if checking the balance of the bank balance with the number of items purchased where the bank balance is greater or equal to the number of transactions, condition (2) transaction file or current account not enough to pay, if checking the balance of the bank balance with the amount of goods purchased where the bank balance is smaller than the number of transactions to be paid.

6. Transaction permission

There is this scenario doing face detect and face an error. Illustrated in figure 25.

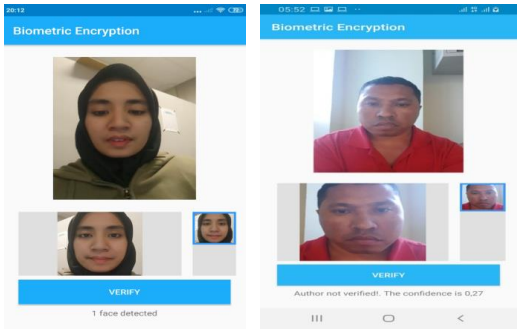


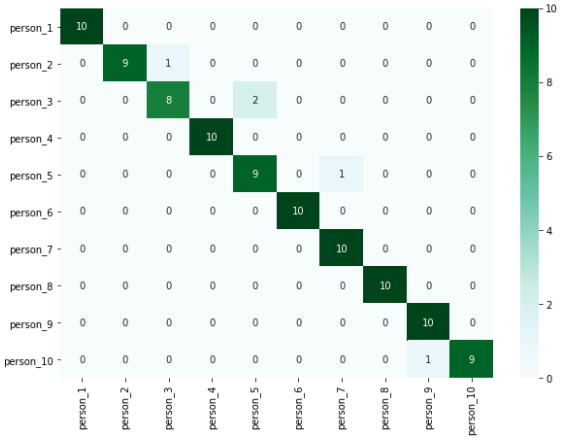
Fig 25. Transaction permission

In the scenario in figure 25 is the result of face detect and face an error. If result face detects, a user has face id in the database cloud server or balance enough between bank and market pay, and QR Code and face id same person. If face error if a user no has face id in the database cloud server or no same QR code and face id different user.

C. Result of transaction permission

In the results of the experimentation permission access transaction of 10 people to analyze the accuracy of the success of the mobile app, the transaction success is done with face recognition. Analysis of the accuracy test in table 1. in an application is said to have high accuracy if it can provide the output of input correctly. In this study, the level of accuracy was measured based on the level of success in re-verifying faces in the same person resulting in true values and different false values on the face..

Table 2. Accuracy transaction permission



Accuracy = (TP + TN) / (TP + TN + FP + FN) = (95X100%) / 100 = 95%.

From table 2, explains that in the experimental of the mobile application for transaction permission with 2 scenarios, (1) using permission transaction face detect with using the same user QR Code and Face, (2) permission transaction face error with transaction permissions with face wrong dan different face user, the experimentation use 10 people samples for experimental. from the experimental results get an accuracy rate of 95%.

D. Time speed transaction experimental

Time speed testing 100 samples experimental for transaction permission for getting the value of average rate. Illustration of experimental time speed in figure 27.

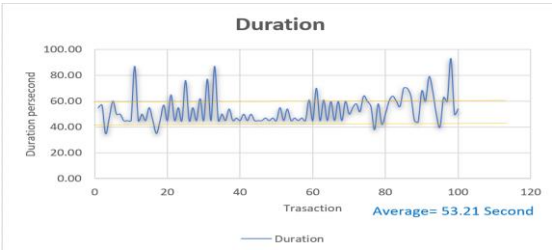


Fig 27. Time speed transaction graphic

From the results of the analysis on time speed in figure 27, it shows that the time needed to perform transactions is only 53.21 second for the per transaction.

CONCLUSION

In this research, build Mobile Platform Biometric Cloud Authentication is a mobile application authentication with biometric to perform permission transactions. Transaction permission uses some data such as QR Code and Face recognizes or verification. Authentication biometrics is authentication by using one part of the human body such as the face, retina, fingerprints, sounds, and others.

The implementation Mobile Platform Biometric Cloud Authentication concept is a 256 bit AES algorithm used for face biometric encryption and decryption. In this research, the implementation use faces recognition or verification.

The transaction permission used is QR Code and face authentication, face data has stored in the cloud server. Mobile apps authentication is built using the Android operating system with a minimum of API Level 22 lollipop.

From the whole of the research on this thesis, it was concluded that:

1. There are two main processes in experimentation is Registration and transaction.
2. Mobile transaction permissions are implemented for merchant transactions and running online access.
3. Registration process using two steps, (1) enrolment user id and face id, (2) create QR Code card.
4. Authentication permission transactions using two steps for authentication, namely (1) with QR Code (2) face verification.
5. Biometric face encryption and decryption with 256 bit AES algorithm.

In the implementation of mobile apps in the transaction permissions process with an accuracy rate of 95% from 10 people experimentation for detect face and error face and with time speed in the average rate per transaction with a time of 23.21 second.

REFERENCE

[1] Badan pusat statistika Indonesia, "tingkat kemiskinan", access February 11 2019. Available: https://www.bps.go.id.

[2] Ahmad Amran, Surya Michrandi Nasution, Fairuz Azmi," Experimentationn of Cryptography Algorithm For Biometric Payment". E-proceeding of engineering, Vol.3, No.1 April 2016.

[3] Tresandern and Timothy F. Cootes," Mobile Biometrics: Combined Face and Voice Verification for the mobile platform", IEEE, Books, 2013.

[4] Selvia Rahmawati1, Ichsan Taufik, Gitarja Sandi," Implementasi Algoritma AES(Advanced Encryption Standard)256Bit Dan Kompresi Menggunakan Algoritma Huffman Pada Aplikasi Voice Recorder", SENTER 2017, 15-16 Desember 2017.

[5] Microsoft Azure,"Face API Azure Cloud documentation" access February 2019.Available:https://www.azure.microsoft.com.

[6] J.Zhou, X.G.Lu, D. Zhang, C. Wu, Orientation analysis for rotated human face detection, Image and Vision Computing, 20, 2002, 257-264.

[7] Weizhi Meng; Wong, D.S.; Furnell, S.; Jianying Zhou,"Surveying the Development of Biometric User Authentication on Mobile Phones," in Communications Surveys & Tutorials, IEEE, vol.17, no.3, pp.1268-1293, third quarter 2015.

[8] Stefan Rass and Daniel Slamanig, "Cryptography for security and privacy in cloud computing", Artech House, Boston London., 2014.

[9] Merchant"online-merchant",access-12-May-2019 . .[online].available:https://www.securionpay.com.

[10] Soyuj Kumar Sahoo and S R Mahadeva Prasanna," Bimodal Biometric Person Authentication Using Speech and Face Under Degraded Condition", IEEE, conf. 28-20 Jan 2011, vol. 5, no. 2, Bangalore, India. 2011.

[11] QR Code, "Basic Understanding of QR Code Payment", access april 22 2019.[online].available: www.molpay.com16.

[12] Omri, F, Foufou, S, Hamila, R dan Jarraya, M," cloud-based mobile system for biometric authentication ,IEEE.2006.

[13] Xudong Cao, Yichen Wei, Fang Wen, Jian Sun," Face Alignment By Explicit Shape Regression", Int J Comput Vis, April 2014, Volume 107.

[14] Xiaoxue Wang, Yufang Zhang and Huicheng Yang, " A Bimodal Biometric Verification System Based on Fingerprint and Face", EEEI, Conf. 14-16 May 2015, vol. 3 no. 2. Beijing , China 2015.

[15] Xiang Sun, "Green Cloudlet Network: A Sustainable Platform for Mobile Cloud Computing", IEEE, conf. 10 Oct. 2017, vol. 14, no. 2-3, IEEE.2017.

[16] Shichao Guan, Robson Eduardo De Grande, Azzedine Boukerche," A Novel Energy Effcient Platform Based Model to Enable Mobile Cloud

Applications",IEEE, conf. 27-30 June 2016, vol. 6 no. 4. Messina, Italy. 2016.

[17] Milos Stojmenovic, "Mobile Cloud Computing for Biometric Applications", IEEE, conf. 26-28 Sept 2012, vol. 6, no. 5, Melbourne, VIC, Australia, 2012