International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 20, Issue 5 (May. 2024), PP. 237-246

Finger shield ATM – ATM Security System using Fingerprint Authentication

P. Sandhya Rani
Computer Science & Engineering(CS)
(Assistant Professor)
Sphoorthy Engineering College.
(JNTUH)

K. Akshay Rao
Computer Science & Engineering(CS)
(B.Tech, JNTUH)
Sphoorthy Engineering College
(JNTUH)

V. Giridhar
Computer Science & Engineering(CS)
(B.Tech, JNTUH)
Sphoorthy Engineering College
(JNTUH)

B. Aditya
Computer Science & engineering(CS)
(B.Tech, JNTUH)
Sphoorthy Engineering College
(JNTUH)

ABSTRACT
The proliferation of ATM Fraud case in Indonesia is still the main concern for the society especially bank customers. In March 2017, a total loss of 5 billion rupiah was recorded as a result of ATM Frauds. While the only solution which ensures security of ATM machines is a 6-digit PIN, there are still a lot of security cracks that can be used by the criminals to steal customer data and the 6-digit PIN itself. One of the most frequent method of ATM Fraud is skimming. Therefore, the authors bring the concept of
Fingershield ATM, ATM Machine that implements biometric identification in the form of fingerprints which is integrated with smart card and database server. Fingerprint technology is powerful identification because of its unique characteristics of each of the minutiae. Despite the fact that customers have to add additional authentication time around 1.5 seconds for fingerprint verification, the security is much improved and guaranteed. This research will use experimental descriptive method. With this method, hopefully ATM Fraud can be minimized so that the customers can feel more secure while using ATM Machines.
Based on implementation and test results which had been done before, Fingershield ATM functions run well and some security parameters have passed the test, as well as almost all specifications are met.
Keywords— *Fingershield ATM, Fingerprint, Minutiae, Smart Card, Database Server, Skimming.*

Date of Submission: 14-05-2024 Date of Acceptance: 26-05-2024

I. INTRODUCTION

The improvement of a nation is ordinarily corresponding o its temperate and innovative improvement. This can be demonstrated from the insights publicized by Bank Indonesia (BI) that appeared expanding add up to exchange utilizing ATM card each year, with the add up to ostensible for the year 2017 is 6200 Trillion Rupiah.

However, there have been cases where violations are committed utilizing ATM card's current shortcoming. One of the commonly utilized strategy is called skimming, which duplicates the substance of the attractive stripes from an ATM card. This strategy will be bolstered utilizing a Stick capturing strategy, by utilizing a covered up camera or a altered keypad.

Solution for this issue is by presenting a biometrics verification framework on ATM machines. Biometrics confirmation framework utilize human's interesting natural include such as unique finger impression, retina, etc. Unique finger impression verification is chosen since of its solidness over other innovation, and is moderately more common and easier to be used in Indonesia. Thus, it can be very useful for customers.

Fingershield ATM is the product developed by adding an extra security measure, which is fingerprint authentication into its system. By adding fingerprint authentication, ATM card skimming and PIN capturing will not be enough to broke into another's bank account. Furthermore, the technology to steal someone else's fingerprint is not commonly known by public.

This paper will explain the design, implementation, and testing of Fingershield ATM.

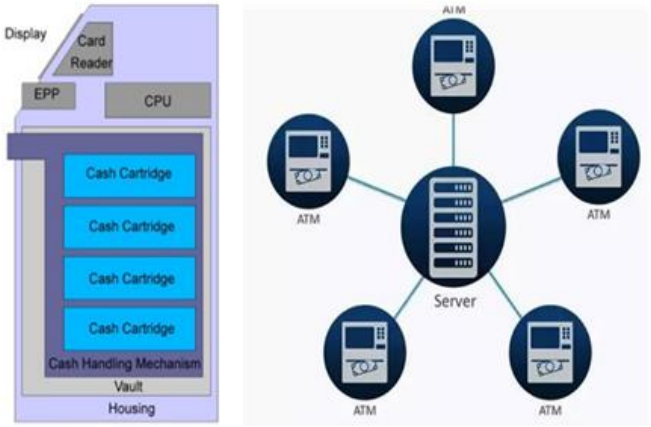
II. FINGERSHIELD ATM

This area will clarify the whole recognize and references utilized amid the work of Fingershield ATM

A. ATM System

ATM Framework comprises of equipment, program, and arrange. ATM Framework is ordinarily made up of the gadgets such as CPU, Card Peruser, Stick, Secure Cryptoprocessor, Show, Record Printer, Vault, Lodging, Sensors and Marker. Nowadays, the endless larger part of ATMs around the world utilize a Microsoft Windows working framework for its computer program, basically Windows XP Proficient or Windows XP Embedded.

Needless to say all ATMs connect to *some* server. This is called the Host Server or Host Switch. The host processor is analogous to an Internet service provider (ISP) in that it is the gateway through which all the various ATM networks become available to the cardholder.



Most have processors can bolster either leased-line or dial-up machines. Leased-line machines interface specifically to the have processor through a four-wire, point-to-point, committed phone line. Dial-up ATMs interface to the have processor through a ordinary phone line utilizing a modem and a toll-free number, or through an Web benefit supplier utilizing a neighborhood get to number dialed by modem.

B. Server

Relational Database Administration Framework (RDBMS) is a sort of database that kept its data in a table, with each push recognizing a certain record, and each column distinguishing a certain field.

To handle an RDBMS database, SQL commands is utilized. Organized Inquiry Dialect (SQL) is a sort of dialect that utilized inquiry to work on a database. There exist a few essential inquiry utilized inside the server subsystem:

- CREATE inquiry to make a modern database
- USE inquiry to utilize a certain database for consequent queries
- SHOW inquiry to appear the substance on an question from a database
- SELECT inquiry to look for a record inside table that coordinated the expression used
- UPDATE inquiry to alter the field esteem in of a record in a table

Within the database server, a few data is scrambled utilizing Progressed Encryption Standard (AES). AES is a sort of symmetrical cryptography. This cryptography utilize a key of 128-bit, 192-bit, or 256-bit sizes. And to scramble the communication, Transport Layer Security (TLS) is utilized. TLS works utilizing a symmetrical cryptography when communicating the information, and utilize topsy-turvy cryptography to confirm users.

C. Smart Card

Smartcard is a chip-tech card that can be utilized as a memory card or chip card. Smartcard is separated into 2 sorts when we conversation around how to utilize them, that are contact and contatcless smartcard. For information transmission, smartcards utilize a convention called APDU (application convention information unit). smartcard can be gotten to with APDU command, and smartcard provide reaction in the frame of APDU reaction. The figure underneath is a construction

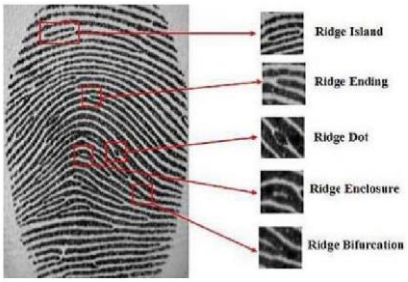
of the APDU command and the APDU reaction. APDU arrange alludes to ISO / IEC 7816 documents.

D. Fingerprint

Fingerprint is a particular design of edges and valleys on the finger surface of an person. A edge is characterized to be a single bended portion though a valley is the zone between two adjoining ridges.

Minutiae focuses are the major highlights of a unique mark picture and are utilized in the coordinating of fingerprints. These particulars focuses are utilized to decide the uniqueness of a unique finger impression picture. A great quality unique mark picture can have 25 to 80 particulars depending on the unique finger impression scanner determination and the situation of finger on the sensor.

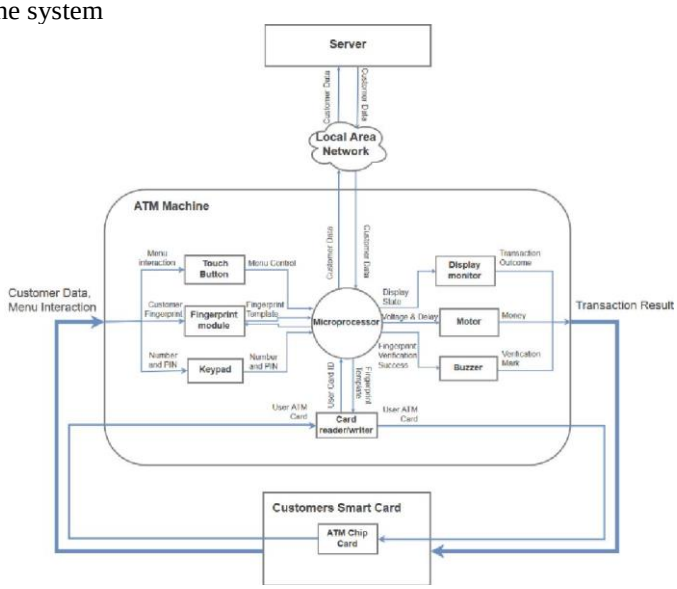
. Edge endings and edge bifurcations are the most commonly utilized minutia sorts since all other sorts of particulars are based on a combination of these two sorts. Figure underneath appears a few of the common particulars patterns.



III. DESIGN

This area will clarify framework prerequisite and steps taking in planning Fingershield ATM. Fingershield ATM needs to satisfy these determinations these specifications.

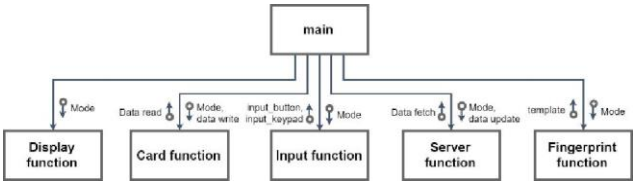
Fingershield ATM design has three main sub-system, i.e. ATM Machine, Server, and Smart Card. Here is the general architecture of the system



Design above used decentralisation method which save fingerprint data in ATM Smart Card instead of server. This design ensures the security in Smart Card and reduce fingerprint verification time and server bandwidth significantly.

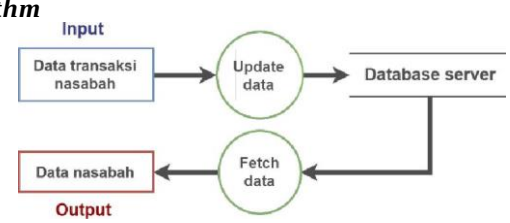
User interaction with system is done with two steps, i.e authentication and transaction. Authentication needs input from user's fingerprint, PIN, and Smart Card. The other user interaction is transaction which includes balance checking, withdraw money, and transfer. All of these feature used server to access user's account. User only needs to choose menu with touch button and input some numbers with keypad. All of this process will be displayed in Monitor and verified by Buzzer. Motor will push the money when user chooses withdraw menu.

A. ATM Machine



There exist five basics functions used by the whole system: display function, card function, input function, server function, and fingerprint function.
Display function is used to show and change the user interface on the display screen. Input function is used to process the keypad input. Card function is used to communicate with the smartcard using the reader, mainly to read and write relevant data. Server function is used to communicate with the database server, to fetch and update data within the database. Fingerprint function is used to do the fingerprint authentication and registration of the user's fingerprint into the bank account.

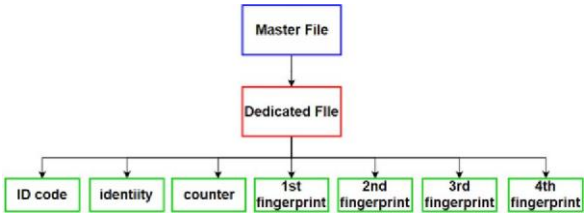
B. Database Server Algorithm



The database server subsystem is comprised of two primary forms: bring information and upgrade information. This work will be utilized to communicate with the database utilizing an SQL query.
Fetch information is a work to bring the current database record values into the client machine. It has 2 modes: get all information field of a record distinguished by card code; and bring a title field of a record recognized by account number for exchange purposes.
Update information is a work to alter the values of areas in a record. It have three modes: to alter the adjust field of a record distinguished by card code for withdrawal purposes; to alter the adjust esteem of a record distinguished by the account number for exchange purposes; and to alter the substantial field esteem of a record for blocking purposes.

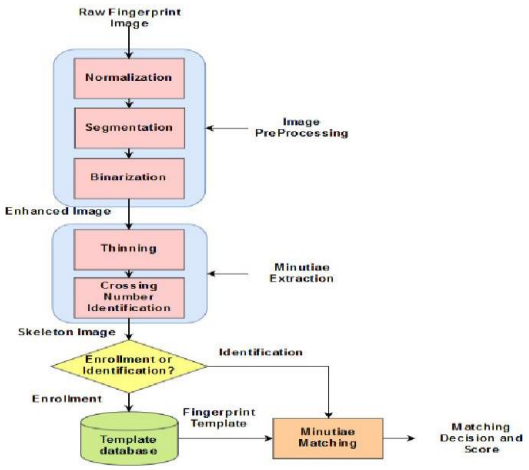
C. Smart Card Algorithm

The figure below explains the data allocation of smartcards used as ATM cards.



In this system, smartcard stores ID code (18 bytes), identity (20 bytes), counter (1 byte) and 4 different fingerprint data from user. In order to access the data, a data flow scheme is required with an explanation as shown below
In the system used, the data entered on the smartcard is a command APDU, then smartcard will generate a response in the form of APDU response. The APDU commands used in this design are the directory access commands, file writing commands, and file readout commands. for more details, the command below is an illustration of each APDU command used in this design.
When the process of writing, the first thing to do is to select the directory where the file is located. Then, when it is in the correct directory, the next thing to do is to write it in the directory. When reading process, similar to when writing data, directory selection is the thing done before the process of reading begins, after which the data reading takes place. The indication of whether the process is successful or not is the APDU response obtained from each command.

D. Fingerprint Algorithm



Processes above are what happened inside fingerprint sensor. First, fingerprint image is captured in grayscale. Raw Fingerprint Image is converted to binary form (Black-White). After that, the image will be filtered and thinned to make fingerprint pattern has 1 pixel width. Minutiae of fingerprint is extracted using Crossing Number method. Crossing Number will decide what type of minutiae is detected and where it is located. Finally, Minutiae Matching is done using Euclidean Distance with controlled threshold to decide whether two fingerprints match.

$= \sqrt{2}$ ——————————————— $+ 2$

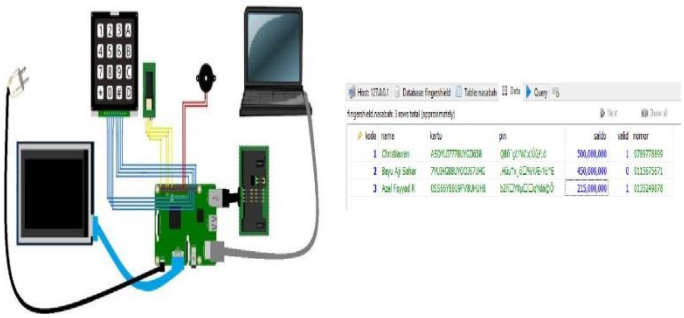
Score is added by one increment with every distance and orientation that fulfil the condition (smaller than maximum threshold).

$$sd\left(m_i, m_j\right) = 1 \Leftrightarrow \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \leq r_0$$

$$dd\left(m_i, m_j\right) = 1 \Leftrightarrow \min\left(\left|\theta_i - \theta_j\right|, 360 - \left|\theta_i - \theta_j\right|\right) < \theta_0$$

IV. IMPLEMENTATION AND TESTING

This section will explain the process of implementing and testing Fingershield ATM



The implementation of Fingershield ATM implementation uses a lot of components with different configuration with microprocessor.

From the figure above, mostly the components use Raspberry Pi GPIO to send and receive voltage. Waveshare Touch Screen Display uses HDMI connection to display image and USB Port for its touch function. Fingerprint communicate with microcontroller using UART. Card Reader communicates with USB Port to read and write. Finally, server which is located in laptop connects to Raspberry Pi via Ethernet cable in order to send and retrieve data.

Fingershield ATM uses a Linux Ubuntu Mate Operating System and Python Programming Language to implement all of its functions.

A. Authentication Process

The program first runs and stayed on idle state until a smartcard is inserted into the reader. Idle display is as shown below

After a smartcard is inserted into the reader, program will prompt for PIN information from the user, which can be inputted using the keypad. On successful PIN authentication, program will then prompt for fingerprint input, which will wait until user put their fingerprint on the sensor. Authentication process is as shown below

On successful authentication, user will then enter the main transaction menu available. On the other hand, user will be prompted for repetition for unsuccessful authentication.

B. Transaction Process

Figure below will show the contents of the database server, and the account used to text will be the one under the name 'Azel Fayyad R'.

Fig.13 Initial Database Records

When balance check menu is picked, then user will be shown their current balance on the display screen with the balance value according to the database.
If user withdraws 100.000 Rupiah using the withdrawal menu, prompted by the screen as shown below, a success message will be displayed on the screen. After that, corresponding amount of money will be dispensed from the slot, and their bank account's balance will be reduced by the same amount of money.

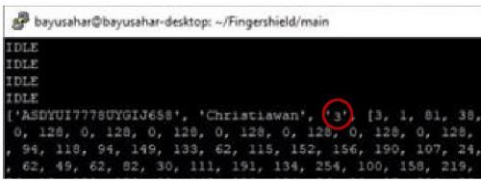
On successful transaction, a success message is displayed and both user's bank account will have its balanced changed accordingly.

Fig.15 Withdrawal Success

C. Card Blocking

ATM card blocking occurs in 2 forms, the first is manual blocking and the other is automatic blocking. Any form of blocking has a different method Manual blocking occurs when an ATM card is manually blocked by the server caused by user reports. When the manual blocking, the valid variable on the server will be worth 0. For more details here is a server view image with an illustration of blocking the card from Christiawan account.

Automatic blocking occurs due to failure to verify PIN 3 times or failure to verify fingerprint nine times in sequence. Counter variable on the ATM card will increase every three times the failure of the fingerprint verification process. then when the counter is worth 3, then the ATM card will automatically be blocked. The following is a counter display on ATM cards



D. Fingerprint Security

There are a lot of fingerprint security in this system. One of them is template data for fingerprint. It could be seen below

Template packet 1 = [0xef01, 0xffffffff, 0x2, 0x82, 0x3, 0x1, 0x5a, 0x1c, 0x75, 0x0, 0xff, 0xfe, 0xff, 0xfe, 0xff, 0xfe, 0xf0, 0x0, 0xc0, 0x0, 0x80, 0x0, 0x80, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x77, 0x16, 0x45, 0xb6, 0x36, 0x99, 0x94, 0xfe, 0x2d, 0xa6, 0x12, 0x3e, 0x23, 0x2a, 0xd0, 0x1e, 0x8, 0x33, 0xce, 0x1e, 0x28, 0x17, 0x54, 0x1f, 0x62, 0x97, 0xd9, 0x3f, 0x29, 0x9c, 0xd2, 0x7f, 0x49, 0x9f, 0x96, 0x5f, 0x73, 0x22, 0x45, 0x3f, 0x4d, 0xa7, 0x16, 0x9f, 0x47, 0x2c, 0x54, 0xbf, 0x26, 0x33, 0xcd, 0x1f, 0x1c, 0xb4, 0xcd, 0x7f, 0x66, 0x38, 0x5b, 0xff, 0x71, 0xb9, 0xdd, 0x5f, 0x63, 0xc3, 0xc1, 0x9f, 0x5e, 0x9d, 0x59, 0x3c, 0x285b]

Fingerprint sensor will produce fingerprint template data according to ANSI/INCITS 377,388-2004 Standard. Then, Fingerprint template is encoded with hexadecimal encryption used by fingerprint sensor so that people cannot easily duplicate template data without using the same sensor

As in template data, security also comes with FAR (*False Accepting Rate*) and verification result. A good fingerprint sensor has <0,001% FAR to ensure that totally different pair of fingerprint is not match. Below is the result of fingerprint verification test and error test.

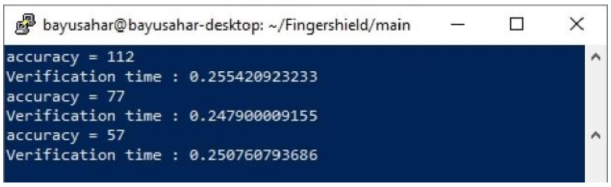


TABLE I
FAR DAN FFR

Threshold	FAR	FFR
0	0	0.06
25	0	0.1
50	0	0.33
75	0	0.67
100	0	0.8

Figure and table above shows that even with zero threshold, not a single fingerprint considered as a false match. However, as the threshold increased, FRR is also increased which indicate false non-matching in fingerprint verification. User needs to put his finger very accurate to be considered as a match fingerprint. Verification scores are also decreasing when users don't place their finger well in the scanning area. Thus, the criminal can't easily make a copy of user's fingerprint and our system for fingerprint is considered secure.

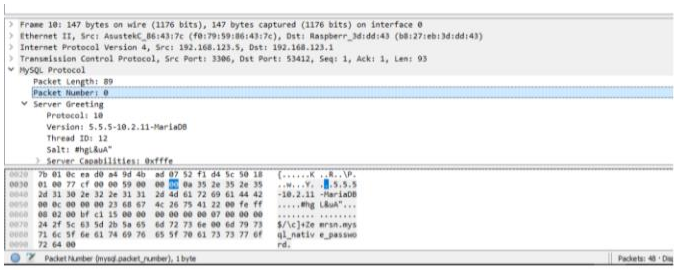
E. Server Security

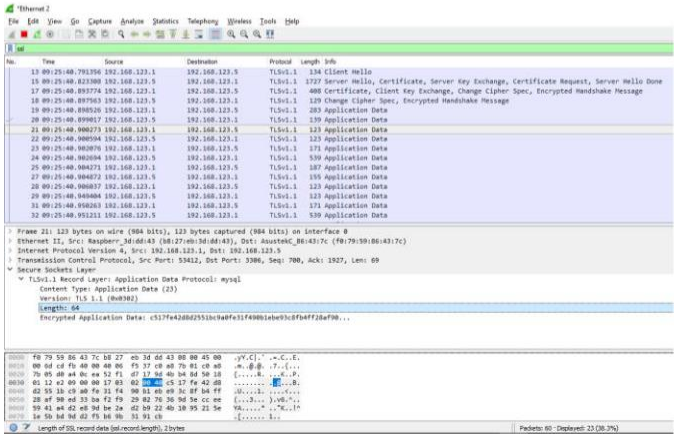
Encryption and decryption is done utilizing standard SQL queries from MySQL. To encrypt PIN information, AES_ENCRYPT() and AES_DECRYPT() queries are used.

Figure above showed that PIN information kept within the database is already in ciphertext that cannot be read normally anymore.

To implement TLS on client-server communication, MySQL feature is used, which is configurable from the settings file to use a specific key. Figure below showed the packets captured on the network interface

Initially, the handshake process is done by the server and client, as shown on the packets in the network interface. Subsequent communications are then only done in TLS communication.

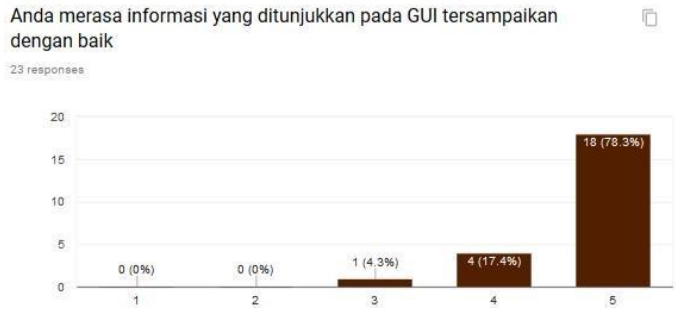




F. User Friendly Testing

23 random people were chosen to test our product and gave their opinion about what they thought after using Fingershield ATM. They used the product without any instructions give and filled the questioner after the test.

The result is shown below



As we can see from the graphs, 95,7% user agreed the information is well delivered from the GUI. User interaction is also easy to understand. Furthermore, 100% user agreed that the GUI is effective and interesting.

For fingerprint technology, 87% user felt it's easy to have a successful fingerprint verification. They only need maximum of 2 tries until their fingerprint is recognized. Others said that they need time to adapt the correct position of the fingerprint and they suggest to create a user guide. Thus, Fingershield ATM is considered to be user friendly.

V. CONCLUSION AND FURTHER DEVELOPMENT

From Implementation and Testing Result, we can conclude that all functions and data processing work properly in the system. Fingershield ATM's security is also high enough due to additional fingerprint authentication and the fact that user's personal information is encrypted. Furthermore, a lot of people gave a positive response to the system in terms of convenience and simplicity. Thus, we hope that this system can reduce the number of ATM fraud especially skimming so that user don't have to worry while transacting by using ATM Machines.

For further development, we recommend to use stronger algorithm or different type of fingerprint module for fingerprint authentication in order to add security for fake fingerprints. Moreover, stepper motor is more recommended than DC motor for its stability to push the money out when withdraw transaction is chosen. Finally, different types of detector can be put inside the ATM to ensure its security such as bill detector, seismic sensor, or record printer.

REFERENCES

[1]. Bank Indonesia. Statictics on ATM Card Transaction (Online). https://www.bi.go.id/id/statistik/sistem-pembayaran. Accessed 30th of January 2018 20:00
[2]. Istnick, Anna C. and Emilio Caligaris. ATM Fraud and Security. DIEBOLD. Amerika Serikat (2003)
[3]. Vellani, Karim H. and Mark Batterson. Security Solutions for ATM. Threat Analysis Group (2003)
[4]. Bhanushali, Nisha and Meghna Chapaneria. Fingerprint based ATM System. Journal for Research, Vol 2 Issue 12 pp 33-34 (2017)
[5]. Patil, Mahesh, Sachin.P. ATM Transaction Using Biometric Fingerprint Technology. International Journal of Electronics, Vol 2 (2012)
[6]. Rhydo Labz. R30X Series Fingerprint Indentification Module User Manual. (Online). https://rhydolabz.com/documents/finger-print-module.pdf. Accessed 13th February 2018 19:10
[7]. Secured Command and Protocol 7816 (XIRKA).2017. Xirka Silicon Tec.
[8]. MariaDB. 2012. Basic SQL Statements (Online). https://mariadb.com/kb/en/library/basic-sql-statements/. Accessed 20th of January 23:00