Fingershield ATM – ATM Security System using Fingerprint Authentication

Christiawan[1], Bayu Aji Sahar[2], Azel Fayyad Rahardian[3], Elvayandri Muchtar[4]

[1,2,3]Student, [4]S.T, M.T., [1,2,3,4]Electrical Engineering Program, [4]Electronics Laboratory
[1,2,3,4]School of Electrical Engineering and Informatics, Bandung Institute of Technology
[1,2,3,4]Bandung 40132, Indonesia

[1]christiawan96@yahoo.com, [2]bayusahar7@gmail.com , [3]zeluqa@gmail.com , [4]eva_muchtar@yahoo.com

***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**

I.ʺ INTRODUCTION

The development of a country is usually proportional to its economical and technological development. This can be proven from the statistics publicized by Bank Indonesia (BI) that showed increasing total transaction using ATM card every year, with the total nominal for the year 2017 is 6200 Trillion Rupiah

However, there have been cases where crimes are committed using ATM card's current weakness. One of the commonly used technique is called skimming, which copies the content of the magnetic stripes from an ATM card. This technique will be supported using a PIN capturing method, by using a hidden camera or a tampered keypad.

Solution for this problem is by introducing a biometrics authentication system on ATM machines. Biometrics authentication system utilize human's unique biological feature such as fingerprint, retina, etc. Fingerprint authentication is chosen because of its stability over other technology, and is relatively 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.ʺ FINGERSHIELD ATM

This section will explain the entire acknowledge and references used during the work of Fingershield ATM

A. ATM System

ATM System consists of hardware, software, and network. ATM System is typically made up of the devices such as CPU, Card Reader, PIN, Secure Cryptoprocessor, Display, Record Printer, Vault, Housing, Sensors and Indicator. Today, the vast majority of ATMs worldwide use a Microsoft Windows operating system for its software, primarily Windows XP Professional or Windows XP Embedded.

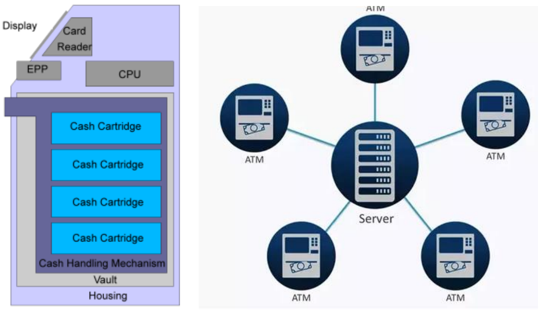


Fig.1 ATM Hardware and Network

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 host processors can support either leased-line or dial-up machines. Leased-line machines connect directly to the host processor through a four-wire, point-to-point, dedicated telephone line. Dial-up ATMs connect to the host processor through a normal phone line using a modem and a toll-free number, or through an Internet service provider using a local access number dialled by modem.

B. Server

Relational Database Management System (RDBMS) is a type of database that kept its information in a table, with each row identifying a certain record, and each column identifying a certain field.

To process an RDBMS database, SQL commands is used. Structured Query Language (SQL) is a type of language that used query to operate on a database. There exist several basic query used within the server subsystem:

- CREATE query to create a new database
- USE query to use a certain database for subsequent queries
- SHOW query to show the contents on an object from a database
- SELECT query to search for a record within table that matched the expression used
- UPDATE query to change the field value in of a record in a table

Within the database server, some information is encrypted using Advanced Encryption Standard (AES). AES is a type of symmetrical cryptography. This cryptography utilize a key of 128-bit, 192-bit, or 256-bit sizes. And to encrypt the communication, Transport Layer Security (TLS) is used. TLS works using a symmetrical cryptography when communicating the data, and use asymmetrical cryptography to authenticate users.

C. Smart Card

Smartcard is a chip-tech card that can be used as a memory card or microprocessor card. Smartcard is divided into 2 types when we talk about how to use them, that are contact and contatcless smartcard. For data transmission, smartcards use a protocol called APDU (application protocol data unit). smartcard can be accessed with APDU command, and smartcard give response in the form of APDU response. The figure below is a schema of the APDU command and the APDU response. APDU format refers to ISO / IEC 7816 documents.

D. Fingerprint

Fingerprint is a distinct pattern of ridges and valleys on the finger surface of an individual. A ridge is defined to be a single curved segment whereas a valley is the area between two adjacent ridges.

Minutiae points are the major features of a fingerprint image and are used in the matching of fingerprints. These minutiae points are used to determine the uniqueness of a fingerprint image. A good quality fingerprint image can have 25 to 80 minutiae depending on the fingerprint scanner resolution and the placement of finger on the sensor.

Ridge endings and ridge bifurcations are the most commonly used minutia types since all other types of minutiae are based on a combination of these two types. Figure below shows some of the common minutiae patterns.

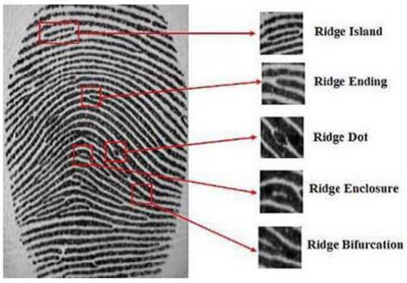
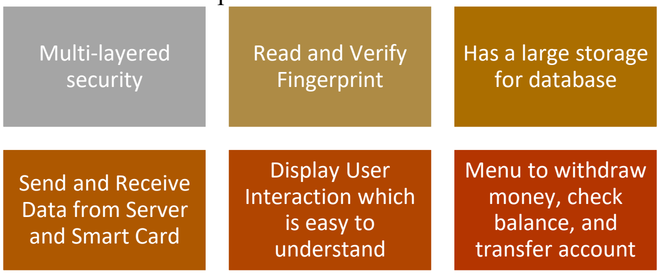


Fig.2 Fingerprint Minutiae Point

III. DESIGN

This section will explain system requirement and steps taking in designing Fingershield ATM. Fingershield ATM needs to fulfil these specifications



Multi-layered security

Read and Verify Fingerprint

Has a large storage for database

Send and Receive Data from Server and Smart Card

Display User Interaction which is easy to understand

Menu to withdraw money, check balance, and transfer account

Fig.3 Specification of Fingershield ATM

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

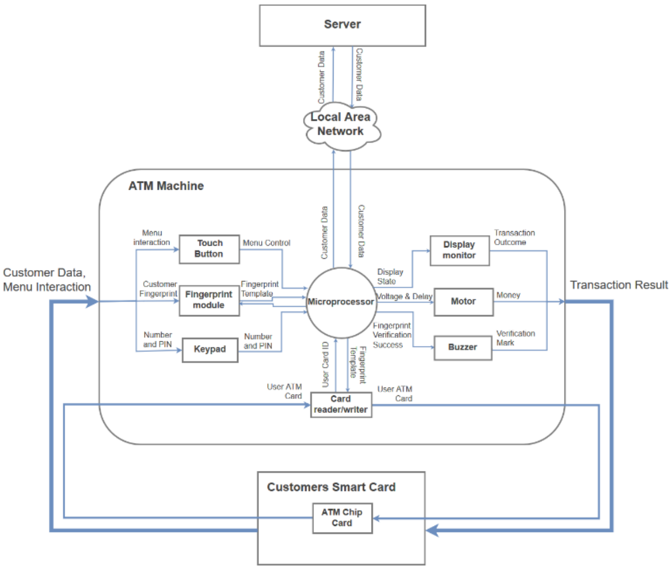


Fig.4 Architecture and Data Flow of Fingershield ATM

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

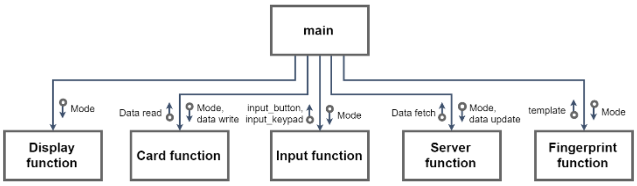


Fig.5 Function List of the Main Program

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

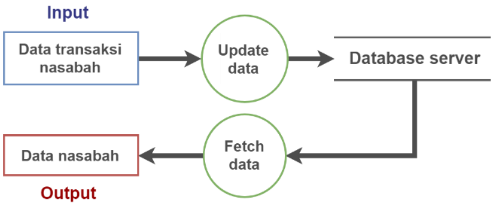


Fig.6 Server Subsystem Dataflow Diagram

The database server subsystem is comprised of two main processes: fetch data and update data. This function will be used to communicate with the database using an SQL query.

Fetch data is a function to fetch the current database record values into the client machine. It has 2 modes: fetch all data field of a record identified by card code; and fetch a name field of a record identified by account number for transfer purposes.

Update data is a function to change the values of fields in a record. It have three modes: to change the balance field of a record identified by card code for withdrawal purposes; to change the balance value of a record identified by the account number for transfer purposes; and to change the valid field value of a record for blocking purposes.

C. Smart Card Algorithm

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

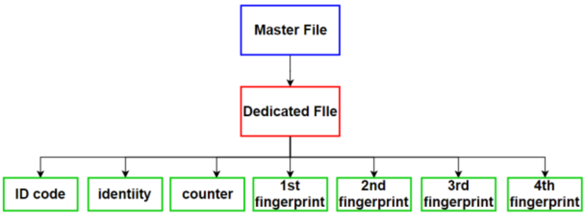


Fig.7 ATM card data

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.

FILE SELECT

CLA	INS	P1	P2	Lc	FILE ID
00	A4	00	00	02	2 bytes

WRITE DATA

CLA	INS	P1 P2(OFSET)	Lc	Data
00	D0	00 00	NN (length)	NN bytes

READ DATA

CLA	INS	P1 P2(OFSET)	Lc
00	B0	00 00	NN (length)

Fig.8 ATM card data

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

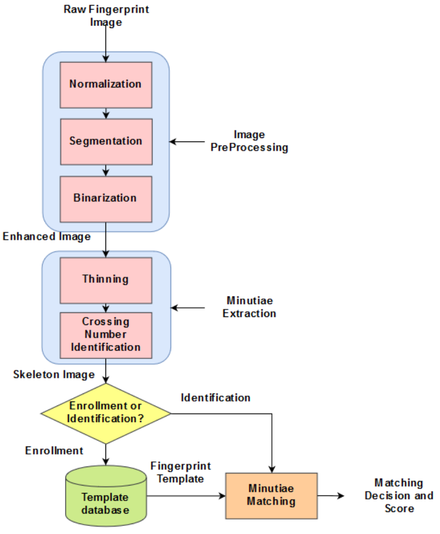


Fig.9 Fingerprint Matching Algorithm

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.

$$CN = 0{,}5\sum^{8} |P_i - P_{i+1}| \text{ with } P_9 = P_1$$

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

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.

$$Ed = \sqrt{dx^2 + dy^2}$$

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

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

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

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. Its connectivity is shown by the figure below

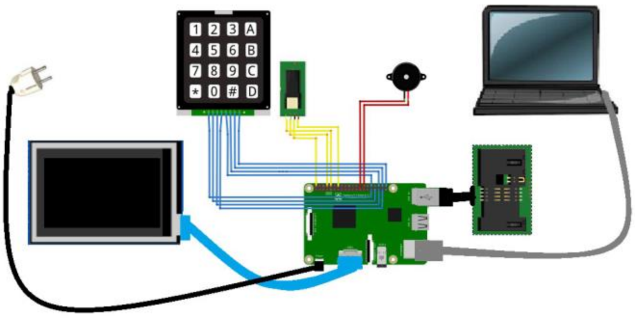


Fig.10 Schematic Circuit of Fingershield ATM

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

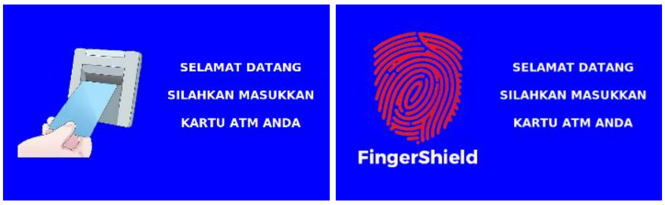


Fig.11 Idle Display

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

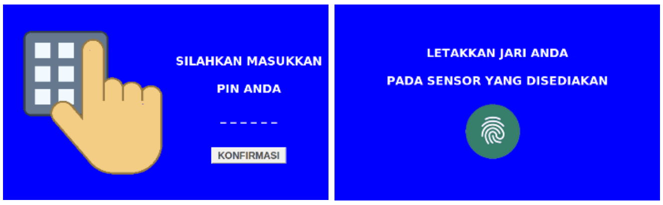
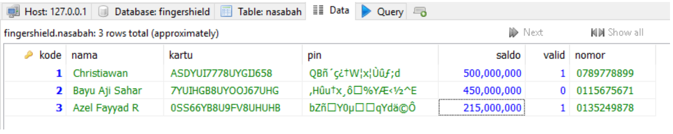


Fig.12 Authentication Process Display

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'.



fingershield.nasabah: 3 rows total (approximately)

kode	nama	kartu	pin	saldo	valid	nomor
1	Christiawan	ASDYUI7778UYGD658	QBñ´ç¿†W¦x¦Ùûƒ;d	500,000,000	1	0789778899
2	Bayu Aji Sahar	7YUIHGB8UYOOJ67UHG	‚Hûu†x¸ô□%YÆ‹½^E	450,000,000	0	0115675671
3	Azel Fayyad R	0SS66YB8U9FV8UHUHB	bZñ□Y0µ□□qYdä©Ô	215,000,000	1	0135249878

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.

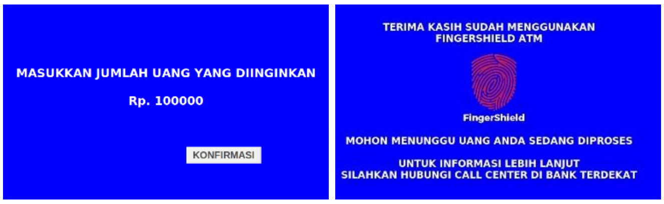

MASUKKAN JUMLAH UANG YANG DIINGINKAN
Rp. 100000
KONFIRMASI
TERIMA KASIH SUDAH MENGGUNAKAN
FINGERSHIELD ATM
FingerShield
MOHON MENUNGGU UANG ANDA SEDANG DIPROSES
UNTUK INFORMASI LEBIH LANJUT
SILAHKAN HUBUNGI CALL CENTER DI BANK TERDEKAT

Fig.14 Balance Withdraw Display

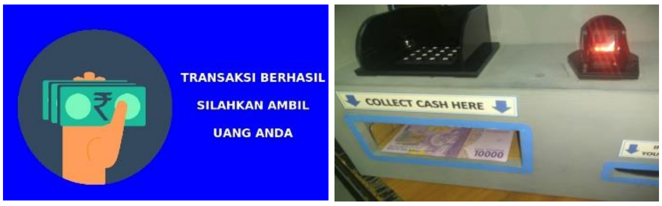
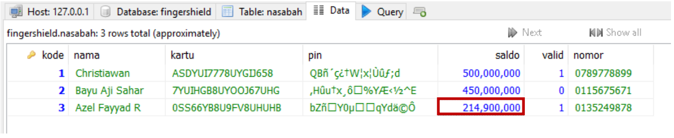


Fig.15 Withdrawal Success



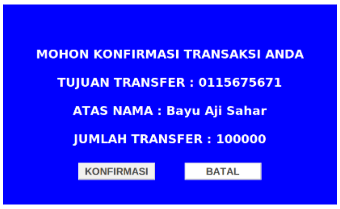
Host: 127.0.0.1 | Database: fingershield | Table: nasabah | Data | Query

fingershield.nasabah: 3 rows total (approximately) Next Show all

kode	nama	kartu	pin	saldo	valid	nomor
1	Christiawan	ASDYUI7778UYGIJ658	QBñ´ç¿†W¦x¦Ùûƒ;d	500,000,000	1	0789778899
2	Bayu Aji Sahar	7YUIHGB8UYOOJ67UHG	‚Hûu†x¸ô□%YÆ‹½^E	450,000,000	0	0115675671
3	Azel Fayyad R	0SS66YB8U9FV8UHUHB	bZñ□Y0µ□□qYdä©Ô	214,900,000	1	0135249878

Fig.16 Database Record After Successful Withdrawal

To test the transfer transation, current user will transfer an amount of money to the target under the name of 'Bayu Aji Sahar'. After a correct input, the transfer summary display is shown and prompts for user confirmation



MOHON KONFIRMASI TRANSAKSI ANDA

TUJUAN TRANSFER : 0115675671

ATAS NAMA : Bayu Aji Sahar

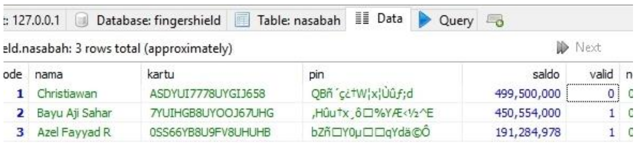
JUMLAH TRANSFER : 100000

Fig.17 Transfer Summary Display

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

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.



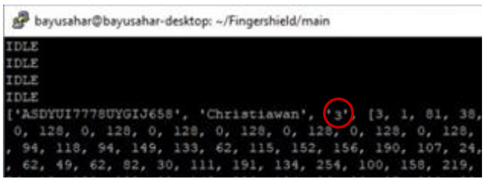
: 127.0.0.1 | Database: fingershield | Table: nasabah | Data | Query

eld.nasabah: 3 rows total (approximately) Next

ode	nama	kartu	pin	saldo	valid	n
1	Christiawan	ASDYUI7778UYGIJ658	QBñ´ç¿†W¦x¦Ùûƒ;d	499,500,000	0	C
2	Bayu Aji Sahar	7YUIHGB8UYOOJ67UHG	‚Hûu†x¸ô□%YÆ‹½^E	450,554,000	1	C
3	Azel Fayyad R	0SS66YB8U9FV8UHUHB	bZñ□Y0µ□□qYdä©Ô	191,284,978	1	C

Fig.18 Manual Bloking

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



bayusahar@bayusahar-desktop: ~/Fingershield/main

```
IDLE
IDLE
IDLE
IDLE
['ASDYUI7778UYGIJ658', 'Christiawan', '3', [3, 1, 81, 38,
 0, 128, 0, 128, 0, 128, 0, 128, 0, 128, 0, 128, 0, 128,
, 94, 118, 94, 149, 133, 62, 115, 152, 156, 190, 107, 24,
, 62, 49, 62, 82, 30, 111, 191, 134, 254, 100, 158, 219,
```

Fig.19 Automatic Blocking

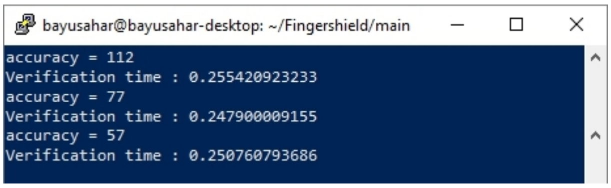
D. Fingerprint Security

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.



bayusahar@bayusahar-desktop: ~/Fingershield/main

```
accuracy = 112
Verification time : 0.255420923233
accuracy = 77
Verification time : 0.247900009155
accuracy = 57
Verification time : 0.250760793686
```

Fig.20 Fingerprint Verification Result

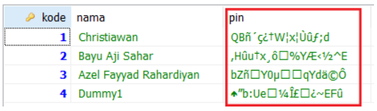
TABLE I
FAR DAN FFR

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.

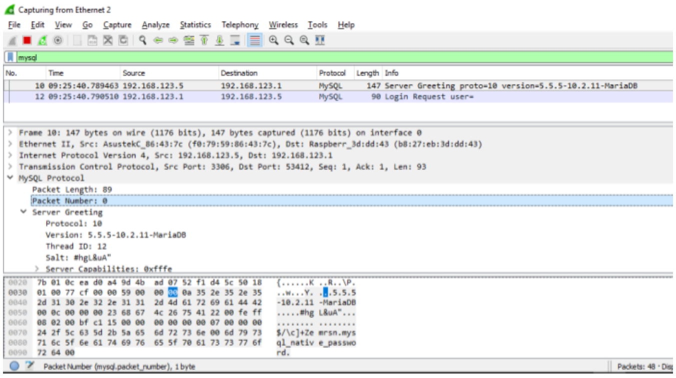


kode	nama	pin
1	Christiawan	QBñ´ç¿†W¦x¦Ùûƒ;d
2	Bayu Aji Sahar	‚Hûu†x¸ô□%YÆ‹½^E
3	Azel Fayyad Rahardiyan	bZñ□Y0µ□□qYdä©Ô
4	Dummy1	♠"b:Ue□¼Î£□¿~EFû

Fig.21 Encrypted PIN Information

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.


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
mysql

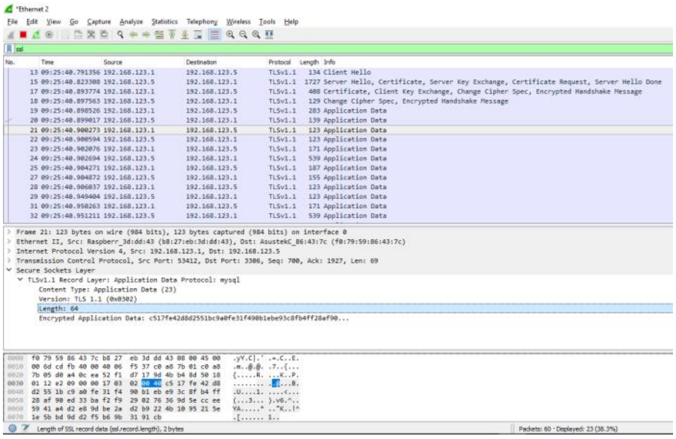
```
No.   Time            Source          Destination     Protocol  Length Info
   10 09:25:40.789463 192.168.123.5   192.168.123.1   MySQL        147 Server Greeting proto=10 version=5.5.5-10.2.11-MariaDB
   12 09:25:40.790510 192.168.123.1   192.168.123.5   MySQL         90 Login Request user=

> Frame 10: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface 0
> Ethernet II, Src: AsustekC_86:43:7c (f0:79:59:86:43:7c), Dst: Raspberr_3d:dd:43 (b8:27:eb:3d:dd:43)
> Internet Protocol Version 4, Src: 192.168.123.5, Dst: 192.168.123.1
> Transmission Control Protocol, Src Port: 3306, Dst Port: 53412, Seq: 1, Ack: 1, Len: 93
v MySQL Protocol
    Packet Length: 89
    Packet Number: 0
  v Server Greeting
      Protocol: 10
      Version: 5.5.5-10.2.11-MariaDB
      Thread ID: 12
      Salt: #hgL&uA"
    > Server Capabilities: 0xfffe

0020  7b 01 0c ea d0 a4 9d 4b  ad 07 52 f1 d4 5c 50 18   {......K ..R..\P.
0030  01 00 77 cf 00 00 59 00  00 00 0a 35 2e 35 2e 35   ..w...Y. ...5.5.5
0040  2d 31 30 2e 32 2e 31 31  2d 4d 61 72 69 61 44 42   -10.2.11 -MariaDB
0050  00 0c 00 00 00 23 68 67  4c 26 75 41 22 00 fe ff   .....#hg L&uA"...
0060  08 02 00 bf c1 15 00 00  00 00 00 00 07 00 00 00   ........ ........
0070  24 2f 5c 63 5d 2b 5a 65  6d 72 73 6e 00 6d 79 73   $/\c]+Ze mrsn.mys
0080  71 6c 5f 6e 61 74 69 76  65 5f 70 61 73 73 77 6f   ql_nativ e_passwo
0090  72 64 00                                           rd.

Packet Number (mysql.packet_number), 1 byte                    Packets: 48 · Dis
```

Fig.22 Handshake Process by the Server and Client


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl

```
No.   Time            Source          Destination     Protocol  Length Info
   13 09:25:40.791356 192.168.123.1   192.168.123.5   TLSv1.1      134 Client Hello
   15 09:25:40.823308 192.168.123.5   192.168.123.1   TLSv1.1     1727 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
   17 09:25:40.893774 192.168.123.1   192.168.123.5   TLSv1.1      408 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   18 09:25:40.897563 192.168.123.5   192.168.123.1   TLSv1.1      129 Change Cipher Spec, Encrypted Handshake Message
   19 09:25:40.898526 192.168.123.1   192.168.123.5   TLSv1.1      283 Application Data
   20 09:25:40.899017 192.168.123.5   192.168.123.1   TLSv1.1      139 Application Data
   21 09:25:40.900273 192.168.123.1   192.168.123.5   TLSv1.1      123 Application Data
   22 09:25:40.900594 192.168.123.5   192.168.123.1   TLSv1.1      123 Application Data
   23 09:25:40.902076 192.168.123.1   192.168.123.5   TLSv1.1      171 Application Data
   24 09:25:40.902694 192.168.123.5   192.168.123.1   TLSv1.1      539 Application Data
   25 09:25:40.904271 192.168.123.1   192.168.123.5   TLSv1.1      187 Application Data
   27 09:25:40.904872 192.168.123.5   192.168.123.1   TLSv1.1      155 Application Data
   28 09:25:40.906037 192.168.123.1   192.168.123.5   TLSv1.1      123 Application Data
   29 09:25:40.949404 192.168.123.5   192.168.123.1   TLSv1.1      123 Application Data
   31 09:25:40.950263 192.168.123.1   192.168.123.5   TLSv1.1      171 Application Data
   32 09:25:40.951211 192.168.123.5   192.168.123.1   TLSv1.1      539 Application Data

> Frame 21: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0
> Ethernet II, Src: Raspberr_3d:dd:43 (b8:27:eb:3d:dd:43), Dst: AsustekC_86:43:7c (f0:79:59:86:43:7c)
> Internet Protocol Version 4, Src: 192.168.123.1, Dst: 192.168.123.5
> Transmission Control Protocol, Src Port: 53412, Dst Port: 3306, Seq: 700, Ack: 1927, Len: 69
v Secure Sockets Layer
  v TLSv1.1 Record Layer: Application Data Protocol: mysql
      Content Type: Application Data (23)
      Version: TLS 1.1 (0x0302)
      Length: 64
      Encrypted Application Data: c517fe42d8d2551bc9a0fe31f490b1ebe93c8fb4ff28af90...

0000  f0 79 59 86 43 7c b8 27  eb 3d dd 43 08 00 45 00   .yY.C|.' .=.C..E.
0010  00 6d cd fb 40 00 40 06  f5 37 c0 a8 7b 01 c0 a8   .m..@.@. .7..{...
0020  7b 05 d0 a4 0c ea 52 f1  d7 17 9d 4b b4 8d 50 18   {.....R. ...K..P.
0030  01 12 e2 09 00 00 17 03  02 00 40 c5 17 fe 42 d8   ........ .@...B.
0040  d2 55 1b c9 a0 fe 31 f4  90 b1 eb e9 3c 8f b4 ff   .U....1. ....<...
0050  28 af 90 ed 33 ba f2 f9  29 02 76 36 9d 5e cc ee   (...3... ).v6.^..
0060  59 41 a4 d2 e8 9d be 2a  d2 b9 22 4b 10 95 21 5e   YA.....* .."K..!^
0070  1e 5b bd 9d d2 f5 b6 9b  31 91 cb                  .[...... 1..

Length of SSL record data (ssl.record.length), 2 bytes         Packets: 60 · Displayed: 23 (38.3%)
```

Fig.23 TLS Communication

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

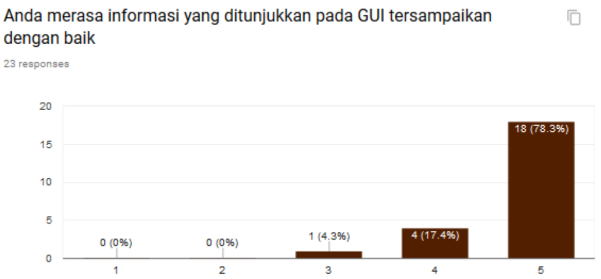

Anda merasa informasi yang ditunjukkan pada GUI tersampaikan dengan baik

Fig.24 User Friendly Graphs for Interface

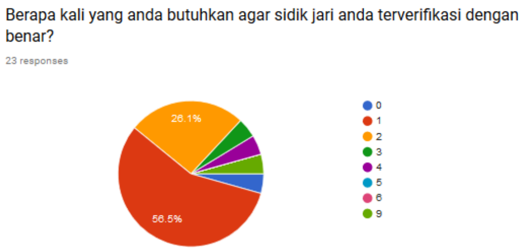

Berapa kali yang anda butuhkan agar sidik jari anda terverifikasi dengan benar?

Fig.25 User Friendly Graphs for Fingerprint

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