Fingerprint Based ATM Security using IoT and Theft Detection

P. Kowasalya, R. Mythili, G. Pavithra, P. Saravanan, Dr. V. S. Arulmurugan

UG Student, Department of ECE, Excel College of Engineering and Technology, Namakkal, India

Abstract:
The proliferation of ATM Fraud case in Indonesia is nonetheless the essential subject for the society in particular financial institution customers. In March 2017, a whole loss of 5 billion rupiah used to be recorded as a end result of ATM Frauds. While the solely answer which ensures safety of ATM machines is a 6-digit PIN, there are nevertheless a lot of safety cracks that can be used by using the criminals to steal client facts and the 6-digit PIN itself. One of the most popular technique of ATM Fraud is skimming. Therefore, the authors deliver the thinking of Fingershield ATM, ATM Machine that implements biometric identification in the shape of fingerprints which is built-in with clever card and database server. Fingerprint science is effective identification due to the fact of its special traits of every of the minutiae. Despite the reality that clients have to add extra authentication time round 1.5 seconds for fingerprint verification, the protection is plenty multiplied and guaranteed. This lookup will use experimental descriptive method. With this method, with any luck ATM Fraud can be minimized so that the customers can experience greater impenetrable whilst the use of ATM Machines. Based on implementation and take a look at effects which had been achieved before, Fingershield ATM features run properly and some protection parameters have handed the test, as properly as nearly all specs are met.

Keywords: Fingershield ATM, Fingerprint, Minutiae, Smart Card, Database Server, Skimming.

I. INTRODUCTION

The improvement of a usa is normally proportional to its low in cost and technological development. This can be verified from the information publicized with the aid of Bank Indonesia (BI) that confirmed growing complete transaction the use of ATM card each and every year, with the complete nominal for the yr 2017 is 6200 Trillion Rupiah. However, there have been instances the place crimes are dedicated the usage of ATM card’s modern-day weakness. One of the oftentimes used method is referred to as skimming, which copies the content material of the magnetic stripes from an ATM card. This approach will be supported the use of a PIN taking pictures method, by way of the use of a hidden digicam or a tampered keypad. Solution for this trouble is through introducing a biometrics authentication gadget on ATM machines. Biometrics authentication machine make use of human’s special organic function such as fingerprint, retina, etc. Fingerprint authentication is chosen due to the fact of its steadiness over different technology, and is quite extra frequent and less difficult to be used in Indonesia. Thus, it can be very beneficial for customers. Fingershield ATM is the product developed with the aid of including an more protection measure, which is fingerprint authentication into its system. By including fingerprint authentication, ATM card skimming and PIN taking pictures will no longer be ample to broke into another’s financial institution account. Furthermore, the science to steal any person else’s fingerprint is now not often recognised via public. This paper will provide an explanation for the design, implementation, and trying out of Fingershield ATM.

II. FINGERSHIELD ATM

This part will give an explanation for the complete well known and references used at some point of the work of Fingershield ATM.

A. ATM System

ATM System consists of hardware, software, and network. ATM System is generally made up of the units such as CPU, Card Reader, PIN, Secure Crypto processor, Display, Record Printer, Vault, Housing, Sensors and Indicator. Today, the full-size majority of ATMs international use a Microsoft Windows running device for its software, specifically Windows XP Professional or Windows XP Embedded.

Figure 1. ATM Hardware and Network

Needless to say all ATMs join to some server. This is referred to as the Host Server or Host Switch. The host processor is analogous to an Internet carrier company (ISP)....
in that it is the gateway thru which all the a number ATM networks emerge as handy to the cardholder. Most host processors can help both leased-line or dial-up machines. Leased-line machines join immediately to the host processor thru a four-wire, point-to-point, devoted phone line. Dial-up ATMs join to the host processor via a regular smartphone line the use of a modem and a toll-free number, or thru an Internet provider company the use of a nearby get entry to range dialled with the aid of modem.

B. Server
Relational Database Management System (RDBMS) is a kind of database that saved its facts in a table, with every row figuring out a positive record, and every column figuring out a positive field. To manner an RDBMS database, SQL instructions is used. Structured Query Language (SQL) is a kind of language that used question to function on a database. There exist countless fundamental question used inside the server subsystem:

- CREATE question to create a new database
- USE question to use a positive database for subsequent queries
- SHOW question to exhibit the contents on an object from a database
- SELECT question to search for a document inside desk that matched the expression used
- UPDATE question to trade the subject price in of a document in a table.

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

C. Smart Card
Smartcard is a chip-tech card that can be used as a reminiscence card or microprocessor card. Smartcard is divided into 2 sorts when we discuss about how to use them, that are contact and contactless smartcard. For information transmission, smartcards use a protocol known as APDU (application protocol records unit). smartcard can be accessed with APDU command, and smartcard provide response in the shape of APDU response. The parent beneath is a schema of the APDU command and the APDU response. APDU structure refers to ISO / IEC 7816 documents.

D. Fingerprint
Fingerprint is a awesome sample of ridges and valleys on the finger floor of an individual. A ridge is described to be a single curved section whereas a valley is the region between two adjoining ridges. Minutiae factors are the most important aspects of a fingerprint photo and are used in the matching of fingerprints. These trivia factors are used to decide the area of expertise of a fingerprint image. A desirable nice fingerprint photograph can have 25 to eighty trivia relying on the fingerprint scanner decision and the placement of finger on the sensor.

![Figure 2. Fingerprint Minutiae Point](image)

Ridge endings and ridge bifurcations are the most typically used minutia sorts considering the fact that all different sorts of trivialities are primarily based on a mixture of these two types. Figure beneath suggests some of the frequent trivialities patterns.

III. DESIGN
This area will give an explanation for machine requirement and steps taking in designing Fingershield ATM. Fingershield ATM desires to fulfil these specs

![Figure 3. Specification of Fingershield ATM](image)

Fingershield ATM plan has three most important sub-system, i.e. ATM Machine, Server, and Smart Card. Here is the prevalent structure of the gadget.

![Figure 4. Architecture and Data Flow of Fingershield ATM](image)
Design above used decentralisation approach which retailer fingerprint facts in ATM Smart Card as a substitute of server. This format ensures the protection in Smart Card and limit fingerprint verification time and server bandwidth significantly. User interplay with gadget is performed with two steps, i.e. authentication and transaction. Authentication desires enter from user’s fingerprint, PIN, and Smart Card. The different consumer interplay is transaction which consists of stability checking, withdraw money, and transfer. All of these function used server to get right of entry to user’s account. User solely wants to pick menu with contact button and enter some numbers with keypad. All of this manner will be displayed in Monitor and validated by way of Buzzer. Motor will push the cash when person chooses withdraw menu.

A. ATM Machine

![Figure 5. Function List Of The Main Program](image1)

There exist 5 fundamentals features used via the total system: show function, card function, enter function, server function, and fingerprint function. Display feature is used to exhibit and trade the person interface on the show screen. Input characteristic is used to manner the keypad input. Card characteristic is used to speak with the smartcard the usage of the reader, frequently to examine and write applicable data. Server characteristic is used to talk with the database server, to fetch and replace information inside the database. Fingerprint feature is used to do the fingerprint authentication and registration of the user’s fingerprint into the financial institution account.

B. Database Server Algorithm

![Figure 6. Server Subsystem Dataflow Diagram](image2)

The database server subsystem is comprised of two primary processes: fetch records and replace data. This feature will be used to speak with the database the use of an SQL query. Fetch facts is a feature to fetch the modern database report values into the customer machine. It has two modes: fetch all records subject of a file recognized through card code; and fetch a title area of a document recognized through account range for switch purposes. Update facts is a feature to exchange the values of fields in a record. It have three modes: to trade the stability subject of a report recognized via card code for withdrawal purposes; to alternate the stability price of a file recognized with the aid of the account quantity for switch purposes; and to alternate the legitimate discipline price of a document for blocking off purposes.

C. Smart Card Algorithm

The discern under explains the records allocation of smartcards used as ATM cards.

![Figure 7. ATM card data](image3)

When the system of writing, the first issue to do is to pick the listing the place the file is located. Then, when it is in the right directory, the subsequent factor to do is to write it in the directory. When studying process, comparable to when writing data, listing choice is the aspect executed earlier than the system of analyzing begins, after which the information analyzing takes place. The indication of whether or not the system is profitable or now not is the APDU response bought from every command.

D. Fingerprint Algorithm

![Figure 9. Fingerprint Matching Algorithm](image4)

Processes above are what came about interior fingerprint sensor. First, fingerprint photo is captured in grayscale. Raw Fingerprint Image is transformed to binary shape (Black-White). After that, the photo will be filtered and thinned to make fingerprint sample has 1 pixel width. Minutiae of fingerprint is extracted the use of Crossing Number method.

\[
CN = 0.5 \sum_{i} |P_i - P_{i+1}| \quad \text{with } P_0 = P_1
\]

When the system of writing, the first issue to do is to pick the listing the place the file is located. Then, when it is in the right directory, the subsequent factor to do is to write it in the directory. When studying process, comparable to when writing data, listing choice is the aspect executed earlier than the system of analyzing begins, after which the information analyzing takes place. The indication of whether or not the system is profitable or now not is the APDU response bought from every command.
Crossing Number will determine what kind of trivialities is detected and the place it is located. Finally, Minutiae Matching is carried out the use of Euclidean Distance with managed threshold to figure out whether or not two fingerprints match.

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

Score is delivered by using one increment with each and every distance and orientation that fulfill the circumstance (smaller than maximum threshold).

$$\text{sd}(m_i, m_j) = 1 - \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq \tau_0$$

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

### IV. IMPLEMENTATION AND TESTING

This part will give an explanation for the method of enforcing and trying out Fingershield ATM. The implementation of Fingershield ATM implement-ation makes use of a lot of elements with distinct configuration with microprocessor. Its connectivity is proven by way of the determine beneath.

**Figure.10. Schematic Circuit of Fingershield ATM**

From the figure above, in general the elements use Raspberry Pi GPIO to ship and acquire voltage. Wave share Touch Screen Display makes use of HDMI connection to show photo and USB Port for its contact function. Fingerprint speak with microcontroller the usage of UART. Card Reader communicates with USB Port to study and write. Finally, server which is positioned in laptop computer connects to Raspberry Pi by Ethernet cable in order to ship and retrieve data. Fingershield ATM makes use of a Linux Ubuntu Mate Operating System and Python Programming Language to put into effect all of its functions.

**A. Authentication Process**

The application first runs and stayed on idle country till a smartcard is inserted into the reader. Idle show is as proven beneath

**Figure.11. Idle Display**

After a smartcard is inserted into the reader, application will immediate for PIN statistics from the user, which can be inputted the use of the keypad. On profitable PIN authentication, software will then instant for fingerprint input, which will wait till consumer put their fingerprint on the sensor. Authentication technique is as proven beneath

**Figure.12. Authentication Process Display**

On profitable authentication, consumer will then enter the fundamental transaction menu available. On the different hand, consumer will be brought on for repetition for unsuccessful authentication.

**B. Transaction Process**

Figure under will exhibit the contents of the database server, and the account used to textual content will be the one underneath the identify ‘Azel Fayyad R’.

**Figure.13. Initial Database Records**

When stability test menu is picked, then consumer will be proven their cutting-edge stability on the show display with the stability cost in accordance to the database. If person withdraws a hundred Rupiah the usage of the withdrawal menu, caused by using the display screen as proven below, a success message will be displayed on the screen. After that, corresponding quantity of cash will be disbursed from the slot, and their financial institution account’s stability will be decreased via the identical quantity of money.

**Figure.14. Balance Withdraw Display**

**Figure.15. Withdrawal Success**
To take a look at the switch transaction, modern-day consumer will switch an quantity of cash to the goal underneath the identify of ‘Bayu Aji Sahar’. After a right input, the switch precis show is proven and prompts for consumer affirmation.

On profitable transaction, a success message is displayed and each user’s financial institution account will have its balanced modified accordingly.

C. Card Blocking

ATM card blocking off takes place in two forms, the first is guide blockading and the different is computerized blocking. Any structure of blocking off has a specific approach Manual blocking off takes place when an ATM card is manually blocked by way of the server prompted by way of consumer reports. When the guide blockading, the legitimate variable on the server will be really worth zero For greater small print right here is a server view photograph with an illustration of blocking off 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 is a lot of fingerprint safety in this system. One of them is template information for fingerprint. It ought to be considered beneath

Fingerprint sensor will produce fingerprint template information in accordance to ANSI/INCITS 377,388-2004 Standard. Then, Fingerprint template is encoded with hexadecimal encryption used by way of fingerprint sensor so that humans can't without problems replica template information barring the use of the equal sensor As in template data, safety additionally comes with FAR (False Accepting Rate) and verification result. A desirable fingerprint sensor has &lt; 0.001% FAR to make certain that completely exceptional pair of fingerprint is now not match. Below is the end result of fingerprint verification take a look at and error test.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>FAR</th>
<th>FFR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0.06</td>
</tr>
<tr>
<td>25</td>
<td>0</td>
<td>0.1</td>
</tr>
<tr>
<td>50</td>
<td>0</td>
<td>0.33</td>
</tr>
<tr>
<td>75</td>
<td>0</td>
<td>0.67</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0.8</td>
</tr>
</tbody>
</table>

Figure and desk above indicates that even with zero threshold, no longer a single fingerprint regarded as a false
match. However, as the threshold increased, FRR is additionally extended which point out false non-matching in fingerprint verification. User wishes to put his finger very correct to be viewed as a suit fingerprint. Verification rankings are additionally reducing when customers don’t area their finger properly in the scanning area. Thus, the crook can’t effortlessly make a replica of user’s fingerprint and our device for fingerprint is viewed secure.

E. Server Security
Encryption and decryption is performed making use of trendy SQL queries from MySQL. To encrypt PIN information, AES_ENCRYPT() and AES_DECRYPT() queries are used.

Figure 21. Encrypted PIN Information

Figure above confirmed that PIN data saved inside the database is already in ciphertext that can’t be examine generally anymore. To put in force TLS on client-server communication, MySQL characteristic is used, which is configurable from the settings file to use a precise key. Figure beneath confirmed the packets captured on the community interface.

Figure 22. Handshake Process by the Server and Client

Figure 23. TLS Communication

Initially, the handshake procedure is carried out through the server and client, as proven on the packets in the community interface. Subsequent communications are then solely performed in TLS communication.

F. User Friendly Testing
23 random humans have been chosen to check our product and gave their opinion about what they thinking after the usage of Fingershield ATM. They used the product barring any guidelines provide and crammed the questioner after the test. The end result is proven beneath

As we can see from the graphs, 95.7% consumer agreed the records is nicely delivered from the GUI. User interplay is additionally effortless to understand. Furthermore, one hundred percent consumer agreed that the GUI is nice and interesting. For fingerprint technology, 87% consumer felt it’s effortless to have a profitable fingerprint verification. They solely want most of two tries till their fingerprint is recognized. Others stated that they want time to adapt the right function of the fingerprint and they advocate to create a person guide. Thus, Fingershield ATM is regarded to be person friendly.

V. CONCLUSION AND FURTHER DEVELOPMENT
From Implementation and Testing Result, we can conclude that all features and information processing work proper in the system. Fingershield ATM’s safety is additionally excessive ample due to extra fingerprint authentication and the truth that user’s private records are encrypted. Furthermore, a lot of humans gave a fine response to the machine in phrases of comfort and simplicity. Thus, we hope that this gadget can minimize the range of ATM fraud particularly skimming so that person don’t have to fear whilst transacting through the use of ATM Machines. For similarly development, we advocate to use superior algorithm or distinctive kind of fingerprint module for fingerprint authentication in order to add safety for faux fingerprints. Moreover, stepper motor is greater endorsed than DC motor for its balance to push the cash out when withdraw transaction is chosen. Finally, distinct kinds of detector can be put inner the ATM to make certain its safety such as consignment detector, seismic sensor, or document printer.

V. REFERENCES


