Enhancing Security Levels In Automatic Teller Machines (ATM) Using Biometric and Multifactor Authentication

Bryan Chau and Binh Le
Department of Computer Science, Georgia State University, Atlanta
nchau1@student.gsu.edu
ble8@student.gsu.edu

***Abstract* — Each individual has various checking/saving accounts in different banks; individuals need to bring numerous ATM cards for purchase, there might be various PINs for each account. Simultaneously, numerous ATM thefts are happening, regardless of whether the CCTV cameras are put in the ATM. The ATM has endured much over the course of the years against PIN theft and other related ATM scams because of its conventional authentication mode (PIN). The purpose of this paper is to propose a multifactor authentication such as a biometric-based fingerprint verification to overcome the security in the traditional ATM systems and protect its user identification.**

***Keywords* — PIN, Fingerprint-based, biometric authentication, Verification, ATM, Multifactor.**

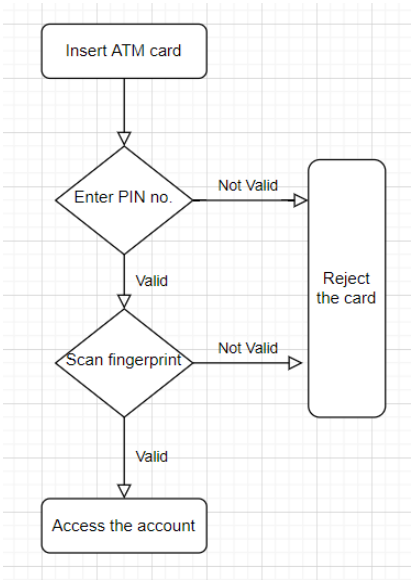
I. INTRODUCTION

An automated teller machine (ATM) is an electronic gadget that replaces a human bank employee. An ATM can play out various fundamental financial systems without direction or mediation by anybody working at the bank institution that possesses the ATM. Some latest ATMs are equipped with mobile cash exchanges. These days Automated Teller machines (ATMs) are broadly utilized due to their easy and speedily accessible money for everybody. Banks provide customers ATM cards, debit cards, or credit cards to make daily transactions. There is

usually a magnetic strip on the back of every card. A magnetic stripe card is a type of pass that permits the user to complete electronic transactions or access a locked physical space. The "stripe" contains embedded information that identifies its user. Types of magnetic stripe cards currently in use include driver's licenses, credit cards, employee ID cards, hotel rooms, gift cards, and public transit cards [1]. With the progress in technologies, there is also the advancement in hackers and criminals in the entire world who are responsible for fraud [2].

This paper proposes a secure, super-fast, and energy-effective ATM banking system that is exceptionally secured compared with the current one. Biometrics-based authentication offers a few benefits over another authentication process; there has been a massive flood in the utilization of biometrics for client verification in later a long time.

II. RELATED WORK



System flow diagram for ATM using Biometric Fingerprint-based

Many countries are using biometrics technology (fingerprint authentication to be precise) and it has been successful to combat ATM frauds by financial organizations such as the Western Bank in the USA, Barclays Bank in the UAE, Groupo Financiero Banorte in Mexico, Banco Falabella in Chile and many more banks around the world are using biometrics [2].

III. PROPOSED METHOD

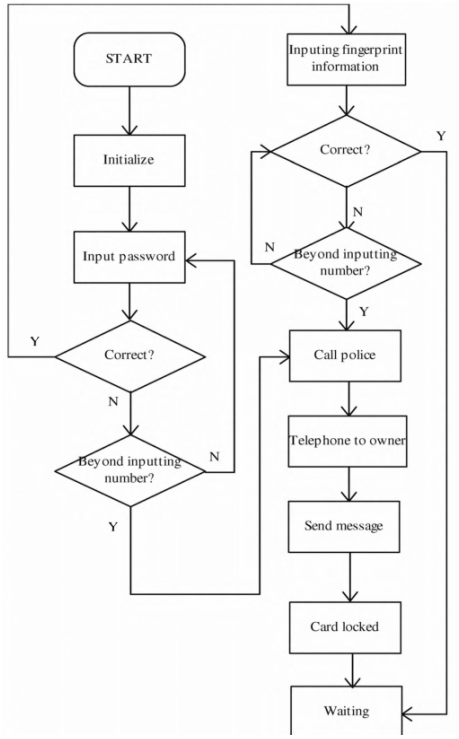
The paper approach for planning a proficient biometric ATM solution for banking exchange is with the end goal that, a person's biometric fingerprint will be scanned and captured when opening a bank account.

This biometric data will be shipped off a third-party biometric merchant (for example, Genkey Solutions), and the merchant will examine the biometric finger impression data and produce BioHASH tokens from them. The BioHASH token is composed of the microchip of a debit or credit card. The biometrics are disposed of after BioHASH tokens have been produced from them.

At the place of authentication or accessing at the ATM, the pre-saved biometric fingerprint on the card and the live fingerprints caught at the ATM are shipped to and being validated in the authentication server securely. This decreases the possibility of a false reject identification and also gives the user more privacy; having his or her biometric information in his or her own custody [3].

Software design

Prior to using the ATM terminal, a password and finger scan are required. First, you need to enter the proprietor's secret phrase; if a personal password is effective, the system requires the proprietor's finger scan. In the event that all the recognition is correct, the system would go into the waiting status. Furthermore, the occasions that recognition of unique fingerprints and passwords are limited to 3. If there are more than three times, the framework will call law enforcement through a police network, phone the proprietor/owner, and send messages to any relevant staff. Then, at that point, the system locked the proprietor's credit card. The overall software chart is below.



Design of fingerprint recognition algorithm

1) fingerprint recognition process

The initial step was securing the finger scan picture by the above device referenced in the algorithms, and the outcomes could be shipped off the accompanying process.

Besides, pre-handling the image acquired. After acquiring the finger scan picture, it should be pre-handling. By and large, pre-processing is separating, histogram processing, image improvement, and image binarization.

Ultimately, the trademark esteem was extracted. The result of the above measures would be analyzed with the data of the proprietor's fingerprint in the database to confirm whether the

person is matched. Afterward, the system returned the outcomes, whether they were verified or not.

2) design of fingerprint image enhancement

The finger impression recognition module is a critical piece of the system; the excellent images were the primary considerations affecting the presentation in the system. The algorithm of finger impression recognition dependent on the algorithm of Gabor was utilized. Fingerprint improvement calculation dependent on the Gabor filter could be more intelligent to eliminate clamor, reinforce the definition between the ridge and valley, and further develop the image improvement handling limit. Yet, this algorithm was delayed in managing the high capacity prerequisites. The algorithm depends on the Gabor filter being utilized in the recoverable area.

The method of Gabor filtering was proposed by Hong et al. [5] and this method is one of the most widely applied to fingerprint image filtering algorithms. The algorithm consists of standardization, direction estimation, frequency estimation, segmentation and filtering steps. The algorithm makes full use of the good directional selectivity of Gabor filtering for image enhancement. The general form of Gabor filter is as follows [6][4]:

$$G(x, y;\ \theta, f) = exp\left\{-\frac{1}{2}\left[\frac{x_{\theta'}^2}{\sigma_x^2} + \frac{y_{\theta}^2}{\sigma_y^2}\right]\right\} \cos(2\pi f x_{\theta})$$

where

$x\theta = x \cos\theta - y \sin\theta$

$y\theta = x \sin\theta + y \cos\theta$

θ is the orientation direction, f is the cosine wave frequency σx and σy is a fixed distance from the Gaussian properties respectively along the x and y-axes.

System design

1) Hardware

A proposed system mixes hardware and software to play out a dedicated task. A portion of the primary gadgets utilized in embedded systems are microprocessors and microcontrollers. This research paper primarily focused on Arduino Uno and Visual Studio. First, we store the customer's fingerprint, and that will be checked with the fingerprint that we are providing at the time of verification. In this proposed system, we use an SQL database to store all the user data. If the fingerprints are authenticated, then the ATM will allow customers to proceed further; in any case, the system will alert.

The errand-related instructions are stacked into Arduino Uno R3, which uses Arduino language. The security framework comprises a unique finger impression module, Arduino Microcontroller Unit, LED pointers, and an alert system and microcontroller that gathers information from the individual fingerprint module.

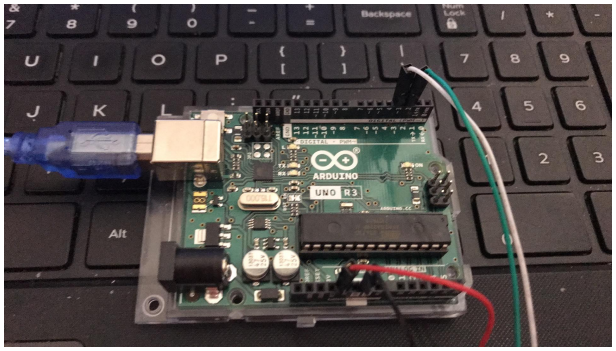


Fig.1. Arduino Uno R3

Our main software depends on this Arduino Uno R3 (Fig.1), which is the most used board among the family of Arduino boards. We are connecting this Arduino board to our fingerprint module.

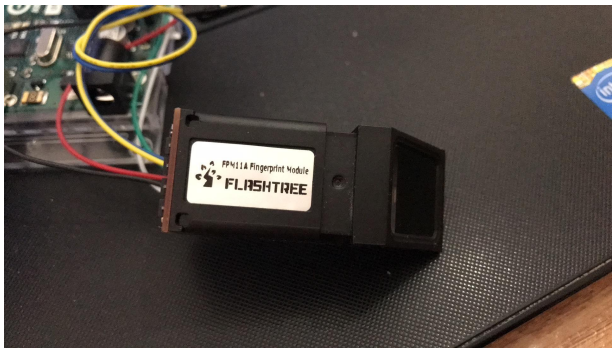


Fig.2. Fingerprint module (front)

Fig.3. Fingerprint module (back)

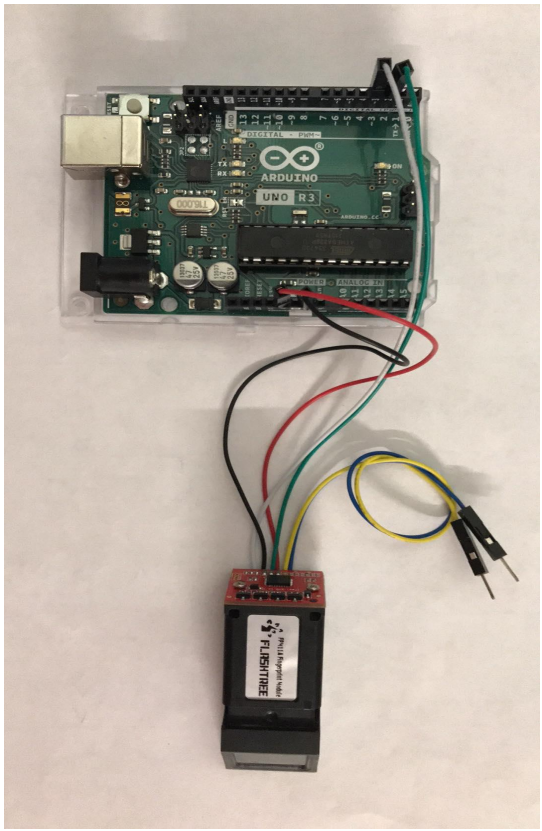
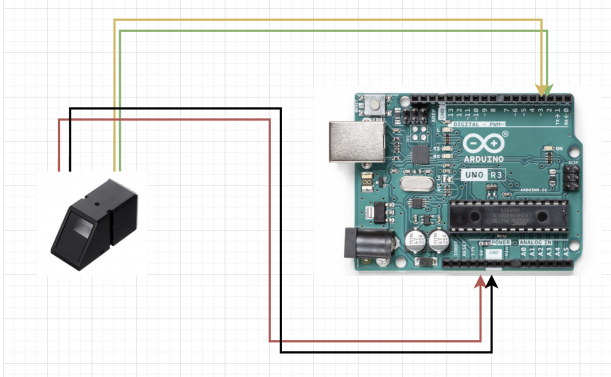


Fig.4. Circuit diagram

We were able to successfully connect our circuit diagram, which is the module we used for our proposed system (Fig.4). We received the fingerprint images from users through the fingerprint module (Fig.2) and the Arduino Uno R3 board. More specifically, the Table.1 below shows the port connection between the Arduino Uno board with the fingerprint module.

Table.1. Port connection from fingerprint module to Arduino Uno R3 board.

Fingerprint Module	Arduino Uno R3
Green Pin	2
White Pin (Yellow)	3
Red Pin	5
Black Pin	GND



With the help of visual studio and SQL we can retrieve the fingerprint from our database that was previously saved.

2) Software and Client-end

In this paper, we made a simple ATM simulation website. Upon using the login page, the user needs to register or scan their fingerprints in order to login using password (Fig.5).

Fig.5. ATM welcome module

After selecting the fingerprint option, the user needs to place his/her finger on the fingerprint scanner in order to verify their identity. Finally, if the user is authenticated, they will be allowed to login using their passwords. If the password exceeds more than 4 times, the ATM card will be locked and the system will alert the local law enforcement and notify its owner.

V. FUTURE WORK

Phase I

The paper tries to propose a flexible design in the future where the client doesn't have to apply a PIN code close by utilizing the biometric unique mark. Besides, all the biometric and biographic data are put away on the debit/credit card. This empowers simple transactions on ATM machines, furthermore, the cardholder doesn't have to memorize PINs and passwords.

Phase II

One essential space of future work is the implementation, also, testing the relative multitude of significant parts of this model plan with a financial organization on a business scale. This will open the project to every one of the practical technicalities in accordance with business use. The papers additionally visualize the float of improvement from an independent application framework to a web application framework utilizing the Model View Controller (MVC) approach.

VI. CONCLUSION

Automatic Teller Machines have turned into an experienced innovation that offers financial assistance to an expanding section of the populace in many nations. Biometrics, specifically individual fingerprint verification, keeps acquiring acknowledgment as a solid type of getting access through identification and authentication processes. The pattern of utilizing biometric information guarantees that the ATMs are secure from distinctive security frauds and attacks. The fingerprint is as yet the most generally used even though it is the most seasoned known biometric innovation.

REFERENCES

[1] Kagan, Julia. “What Is a Magnetic Stripe Card?” *Investopedia*, Investopedia, 26 Aug. 2021, www.investopedia.com/terms/m/magnetic-stripe-card.asp.

[2] A. T. Siddiqui, "Biometrics to Control ATM scams: A study," 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], 2014, pp. 1598-1602, doi: 10.1109/ICCPCT.2014.7054755.

[3] G. A. von Graevenitz, “Biometric Authentication in Relation to Payment Systems and ATMs,” Datenschutz und Datensicherheit - DuD, vol. 31, issue 9, pp. 681-683, September 2007. Online ISSN: 1862-2607. DOI: 10.1007/s11623-007-0223-9.

[4] L. Chen, H. Y. Yin, T. Wang, H. Xu and M. S. Tong, "An Improved Algorithm for Enhancing Fingerprint Image Quality," 2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama), 2018, pp. 371-375, doi: 10.23919/PIERS.2018.8598187.

[5] A. Jain, L. Hong and R. Bolle, "Online fingerprint verification", *IEEE Transactions on*

Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-314, 1997.
[6] G. Feng, G. Gu and B. Zhang, "Fingerprint image preprocessing and feature extraction", *Computer Application Research*, vol. 12, no. 6, pp. 52-57, 1997.