**Project Synopsis**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DEPARTMENT** | Computer Science Engineering | | | |
| **TITLE OF THE PROJECT** | Finger Print Authentication for ATM Card Transactions | | | |
|  |  | | | |
| **STUDENT NAMES/ USN/ PHONE/ MAIL ID** | Osman C | Samarth S K | Ruthwik H P | Vadiraj K R |
| 1DS16CS074 | 1DS16CS096 | 1DS16CS125 | 1DS16CS131 |
| 7795181560 | 7795003350 | 9731802766 | 8861619204 |
| [christopher.osman10@gmail.com](mailto:christopher.osman10@gmail.com) | [s.samarthkulkarni@gmail.com](mailto:s.samarthkulkarni@gmail.com) | [aspire1998@gmail.com](mailto:aspire1998@gmail.com) | [vadikrh@gmail.com](mailto:vadikrh@gmail.com) |
| **PROJECT TIMELINE**  (Tentative Start date- End Date) | August 2019 to May 2020 | | | |
| **PROJECT GUIDE** | Dr. Amutha S | | | |
| **FIELD OF PROJECT** | Cyber Security | | | |

**Introduction**

Authentication is the act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing's identity, authentication is the process of verifying that identity. It might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product or document is not counterfeit.

Authentication is relevant to multiple fields. In art, antiques and anthropology, a common problem is verifying that a given artifact was produced by a certain person or in a certain place or period of history. In computer science, verifying a user's identity is often required to allow access to confidential data or systems.

Authentication can be considered to be of three types:

The first type of authentication is accepting proof of identity given by a credible person who has first-hand evidence that the identity is genuine. When authentication is required of art or physical objects, this proof could be a friend, family member or colleague attesting to the item's provenance, perhaps by having witnessed the item in its creator's possession.

The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph.

The third type of authentication relies on documentation or other external affirmations. In criminal courts, the rules of evidence often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it.

In computer science, a user can be given access to secure systems based on user credentials that imply authenticity. A network administrator can give a user a password, or provide the user with a key card or other access device to allow system access. In this case, authenticity is implied but not guaranteed.

Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Typically, biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices.

Fingerscanning, the digital version of the ink-and-paper fingerprinting process, works with details in the pattern of raised areas and branches in a human finger image.

Finger vein ID is based on the unique vascular pattern in an individual's finger.

Fingerprint recognition is one of the most secure systems because a fingerprint of one person never matches with the others. Bio-metrics authorization proves to be one of the best traits because the skin on our palms and soles exhibits a flow like pattern of ridges on each fingertip which is unique and immutable. This makes fingerprint a unique identification for everyone.

**Literature Survey Summary**

The base paper that we have chosen is “Design and Implementation of a Fingerprint Based Lock System for Shared Access” written by Jayasree Baidya, Trina Saha, Ryad Moyashir and Rajesh Palit.

This paper deals with the design and implementation of a finger based lock system for shared access of a door system. The paper deals with an Arduino UNO component linked to a fingerprint scanner which controls the door lock.

Biometric systems such as fingerprint provide tools to enforce reliable logs of system transactions and protect an individual’s right to privacy. The RFID or password based door lock mechanisms can easily be compromised when the RFID card or passwords are shared or stolen, thus for facilities with shared access require biometric based secure system. In the proposed system, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed and a new user can be enrolled in the system.

The paper fails to deal with the issue of multiple electronic locks and that the end product is quite bulky and so the paper also discusses how the entire system can be improved via Multi-locks, Computerized Fingerprint lock system, Smartphone based fingerprint authentication and so on.

The limitations of this product that this paper states are that the scanner will not be able to detect any fingerprints if the fingerprint has been exposed to any chemicals or damaged. It also cannot deal with dirt particles on the finger as well as any cuts or bruises that show up on the finger of the user. The system implemented cannot also correctly detect the fingers of children due to the constant growth that children go through.

Since this lock needs electricity to run, a power failure can make it totally useless. Thus an UPS or battery is needed. We used relay module, which is sensitive to power it gets. If it does not get sufficient power then relay switching sometimes malfunctions. So we had to give constant power to the relay module. The optical sensor we used is prone to scratches, dirt. As a result it may sometimes give inaccurate result.

**Project Problem Statement and Challenges**

**Problem Statement**

The conventional use of password/PIN is analyzed for security. Although they are found to provide a good level of security, it is noticed that it is not at the required level for the data it is supposed to secure. There are various ways to obtain a PIN or password of another user, a few of them are :

1. Skimming

This method allows the unauthorized person to gain access to the details of the card by using a skimmer and then using a fake keypad to get the PIN effectively compromising the entire account’s security.

1. Cracking

As with most passwords/PINs, the data is hashed and then sent over the intranet/internet to the server. Since passwords and PINs are not unique, cracking of one hash could expose the credentials of more than 1 account.

1. Guessing

Since PINs are usually only 4 digits long it is not a difficult task to guess the PIN, the only prevention of this right now is that the account gets locked after 3 wrong attempts at entering the right PIN

1. Hacking

Some of the online platforms and gateways use the ATM PIN to conduct debit/credit card transaction, if this data is intercepted by a malicious person, the security of the account is compromised.

**Challenges**

The main challenges would be:

1. Installation of the fingerprint sensor in all the ATM stalls across the country.
2. Encrypting of the fingerprint data in the ATM machine.
3. Transmitting a larger amount of data for authorization than passwords/PINs.

**Objectives**

* Specifying requirement for a system involving fingerprint authentication.
* Designing a system for fingerprint authentication.
* Implementing a system for fingerprint authentication.
* Applying the authentication system for ATM card transactions.
* Testing the system for errors and bugs.
* Maintenance of the system.

**Proposed Solution**

Based on the base paper, we will be implementing a system involving fingerprint authentication for ATM card transactions.

The various components that our system requires are, a fingerprint scanner with a USB cable to obtain data on the finger print, and a RFID scanner to scan the credit/debit card to allow the system to know which account is being used.

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person.

The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities.

We plan to implement this system of using fingerprints for authentications purposes using the programming language, C++ with the Adafruit library which is a library used specifically for fingerprint authentication. We plan to implement this system using the platform Visual Studio 2019.

As for the demonstration, we plan to create a web based application using HTML, CSS, JavaScript, VanillaJS, ExpressJS and MongoDB. The demonstration will be to showcase exactly how a transaction between reading the card, to authenticating the transaction in the bank’s server and authorizing the transaction and sending feedback to the customer who used the card and has used his/her fingerprint as authorization of the purchase.

**Platform that will be used for implementation**

**Software tools:** Adafruit library

**Hardware tools:** Fingerprint Scanner, RFID scanner, RFID Tags

**Development Environment:** Visual Studio 2019

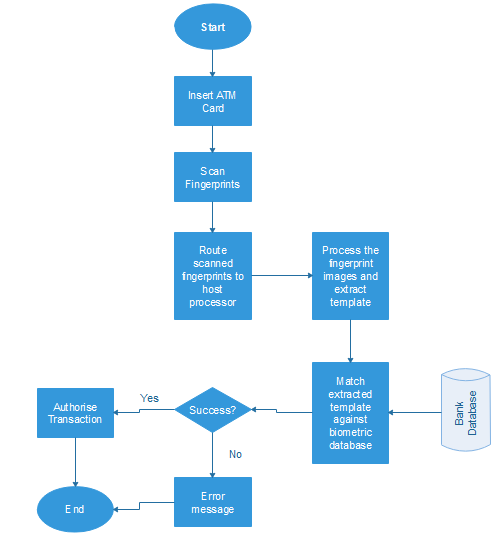
**Programming Language:** C++

**Demonstration details**

We will be using a Web based application which will be implemented using HTML, CSS, JavaScript, VanillaJS, ExpressJS and MongoDB.

The demonstration will consist of a transaction that will occur on a website which will show how the transaction occurs and whether or not the transaction initiated by the account holder or card holder is done by the true owner of the account or card and this is done by cross verifying the data on the fingerprint given during transaction initiation and the fingerprint of the owner that is present in the bank’s database.

**System Diagram**



**Dataset**

Regarding the dataset, depending on our guide’s suggestion and our own knowledge, we would choose to either generate our own dataset or find one on the Internet that relates to our project’s problem statement.

**References**

1. Baidya, J., Saha, T., Moyashir, R. and Palit, R. (2017). Design and Implementation of a Fingerprint Based Lock System for Shared Access. Ph. D. North South University, Dhaka.
2. Mary Lourde R and Dushyant Khosla. Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, 2(5), October, 2010.
3. Zevdin Pala and Nihat Inanc. Smart Parking Applications Using RFID Technology. 1st Annual RFID Eurasia, Istanbul, 2007.
4. Yu-Chih Huang. Secure Access Control Scheme of RFID System Application. Fifth International Conference on Information Assurance and Security, China, 2009.