Volume 9, Issue 3, March – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR375

Mult-Pattern Fingerprint Security System

S. Mangalapriya[1]; Nithyanantham R[2].; Arvindhan G.[3]
Assistant Professor[1]; Research Scholar[2,3]
Veltech High-Tech, Engineering College, Avadi- 600028

Abstract:- To improve security measures, a multi-pattern fingerprint security system is proposed in this study. To offer sophisticated security features, the suggested system combines a database, an Arduino Uno board, and a fingerprint sensor. Because of the way the system is designed, it may keep multiple fingerprint patterns in the database, which adds to its adaptability and versatility.

The Arduino Uno board functions as the client in the proposed system's client-server architecture, while the database serves as the server. The user's fingerprints are captured by the fingerprint sensor, which then transmits the information to the Arduino Uno board for processing. After that, the Arduino Uno board transmits the fingerprint information to the database for authentication and storage. Additionally, the system has a graphical user interface (GUI) that.

Keyword:- *Fingerprint, Arduino, SQL, Multi-Pattern, Security System.*

I. INTRODUCTION

An inventive way to improve security measures is the multi-pattern fingerprint security system. For enhanced security features, this system combines a database, an Arduino Uno board, and a fingerprint sensor. Multiple fingerprint patterns can be kept in the system's database thanks to its design, which boosts the system's adaptability and versatility. The suggested technique is affordable and simple to include into the security systems that are already in place. It can be applied in a number of settings, such as government buildings, banks, and medical facilities, where cutting-edge security measures are crucial.

II. PROBLEM STATEMENT

The numeric security system, or pin-based security system, that is now in use in lockers, ATMs, and other types of protection lacks uniqueness in its digit pattern, making it readily cracked by brute force attack, dictionary search, and other methods. By entering the possibility 1234, we are able to carry out 10% of the possibilities to crack a pin-based security pin, making the possibilities easily crackable and the values of pins not unique. In contrast, the probability of a number between 0 and 9 is increased when 0.01% of 100 people select the same number, indicating that the pin-based system is not unique and is easily crackable. With security system advancements, biometric security.

III. EXISTING SYSTEM

Fingerprint security systems provide numerous services and benefits, including biometric door locks, time and attendance systems, mobile devices, payment systems, and border control. These systems are long-term and continuously used for specific security and purpose-related purposes; however, they also have many drawbacks, including limited applications, privacy and hygiene concerns, and accuracy issues. We tended to develop the suggested system in order to address every problem.

➢ *Disadvantages*

- Absence of variety and originality
- Minimal confirmation of safety or security
- Security can be readily compromised or skewed by employing well-known methods like master prints, brute-force attacks, etc.

IV. PROPOSED SYSTEM

The "Multi-pattern fingerprint security system" that is being suggested improvises the fingerprint recognition process by combining many fingerprints to create a complicated pattern. Consequently, the system makes use of an Arduino UNO board to access the data. Data is gathered from a fingerprint scanner by the user of several fingers in succession, applied, or saved onto the data in a SQL server database, allowing for the modification of The accompanying pictures and code provide a brief explanation of the suggested system. Finger data requires authentication of the individual who has been the user in this instance. Thus, accessibility, cost-effectiveness, and data security are all favored by this breakthrough. Additionally, the system distinguishes the security system greatly from the customary or current system.

V. REQUIREMENT ANALYSIS

A. Software Requirements

An open-source program called the Arduino integrated development environment (IDE) is used to upload programs to any programmable circuit board that can perform a certain function. The IDE is useful for developing programmable code because it has several layouts, such as a sketchbook for writing programs in text using a C++ variant, library management for managing, finding, and updating internal and external libraries to be included in the sketches, serial monitor for monitoring

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR375

serial output, serial plotter for tracking various data, board manager for managing the various boards connected to the uploading device, and debug for identifying and fixing issues in the sketch.

B. Microsoft SQL Server Management Studio

This studio is specifically designed to manage databases for any server or collection of servers. The Microsoft SQL Server Management Studio (SSMS) is an open-source integrated environment used to manage, access, configure, and develop all necessary components of a Microsoft SQL Server, Azure database, Azure VM, and many more. SQL is a structured query language that is used to define, manipulate, and control database records. Embedded SQL, on the other hand, combines the computational power of programming language, like C++ in this case, with SQL's ability to manipulate, define, and control data. SQL statements can be written directly into the source program, or the corresponding programming language. Additionally, SQL Server offers many authentication prompts.The open-source integrated environment development tool Microsoft Visual Studio is used to create computer programs. In this instance, we are using Visual Studio to create a registration page and form page for user manipulation and data entry. We were able to develop a form page by windows form page application (.NET framework) with the aid of Visual Studio. It can collect data from users and store it in the database we built. Additionally, it supports multiple languages and a wide range of project types, including cloud desktop, games, IOT, and many more. Visual Studio also offers applets for every facet of projects.

C. Hardware Requirements

There are various variations of the Arduino programmable circuit board; for this project, we chose the ARDUINO UNO R3 board, which is built on an ATmega328 microprocessor and a detachable dual inline package (DIP). There are 20 digital input/output pins on the Arduino Uno R3 microcontroller, of which 6 are PWM and the remaining 6 are analog. The power source for this microcontroller can come from an AC/DC adapter or a battery that has a voltage between 6 and 20 volts.

The microcontroller Atmega328 uses a maximum of 80mA when it is writing.

With a maximum CPU speed of 20MHz, the ATmega328 microcontroller is an 8-bit AVR RISC microcontroller with 32kb of flash memory and 2kb of SRAM. There are two distinct ATmega328 variants: ATmega328p.

D. Fingerprint Scanner

The optical fingerprint scanner is a device that uses a digital camera to take a 2D image of a fingerprint. The camera passes light over the area where the fingerprint is to be kept, capturing the fingerprint in the 2D image and storing it in the designated storage medium. The scanner's good high resolution is measured in dots per inch (DPI).

Particulars: A fingerprint sensor can store data in the form of a finger image, which is a 2D image, and it can save 127 print spots. Six pins make up a fingerprint sensor; the first pin is used for the power supply, and the second pin is used for the ground signal.

VI. METHODOLOGY

A. Login Forms

We gather information from the user in this portion of the login form, including their preferred password and username. Through development, we were able to store user data in the server-created login database by using the SQL Server Management Studio path. Additionally, we were able to establish a link between the login function and database under the login page, which is coded to gather user data. The user cannot access the authentication area of the security panel until their login is complete. Please refer to figure (1)

B. Registration Catalog

After logging in successfully, the user can access the registration catalog, which is divided into three main sections: the task section, the database grid view, and the registration section. Each section has its own specifications and priority. The user must enter his personal information from the registration area of the page. After enrolling, the user's data will be visible in the database grid view, and the search bar can be used to look up specific users' data. To add new data, the registration process requires adding a fingerprint combination in relation to the user ID. There will be two buttons in the task section: one to save and another to change where.

C. Fingerprint Scan Form

The user will now be able to add his fingerprint to the system using the optical fingerprint sensor once his registration with a unique ID is complete. The ID entered in the registration form will be visible in the biometric data pallet here in the fingerprint storing form. As stated, this is the combination and uniqueness of the security system, and the user will be mentioning his unique number in various aspects below the Redbox available. After entering data into the textbox, the user will be asked to enter his various combinations of fingerprints to complete his enrollment by clicking the scan button below the textbox for each different biometric data. After the user successfully enters his fingerprints, the Redbox will turn into green boxes that resemble in.

D. Fingerprint Checking Form:

This form is primarily used in the section labeled "Data Modification," where users can edit information that will be mirrored into the database after first authenticating themselves using their biometric data in accordance with combinations they provide. The manner of verification is akin to the storing procedure; for every biometric piece of information, the scan button must be pressed in order to confirm the user's biometric combination and to authenticate subsequent operations,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR375

including adding new data or removing old data. Please see figure (1)

VII. SYSTEM DESIGN

A. Architectural Design

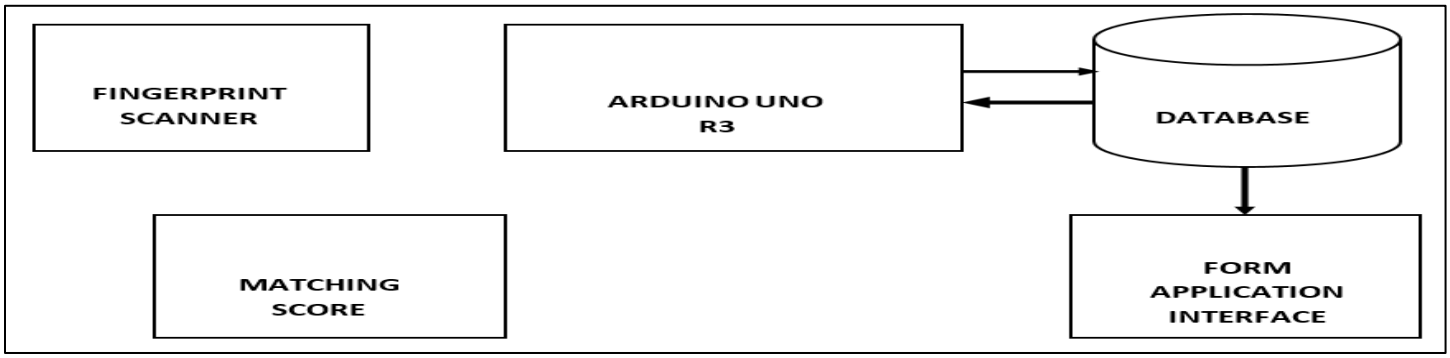

Fig 1: Workflow of the System

This is the project's architectural or model design. This is similar to the process workflow, in which the user provides fingerprint data, which is processed by an Arduino board. The data is then stored in a database for each process, including updating and deleting information. The process then opens up to verify the user's identity by going back to the earlier step, where the form application interface carries out all of the instructions given to the user.

B. Login Form

This is the login form, where the user needs to enter the correct password and username in order to log in. This is the login page where the system identifies any users that have been allocated to it. As a result, the user's information (username and password) is saved in the database, which is displayed on page 26 (picture 2).

These programs are created using Visual Studio, which is referred to as a Windows application because each page is created with a specific function in mind.

C. Registration Form

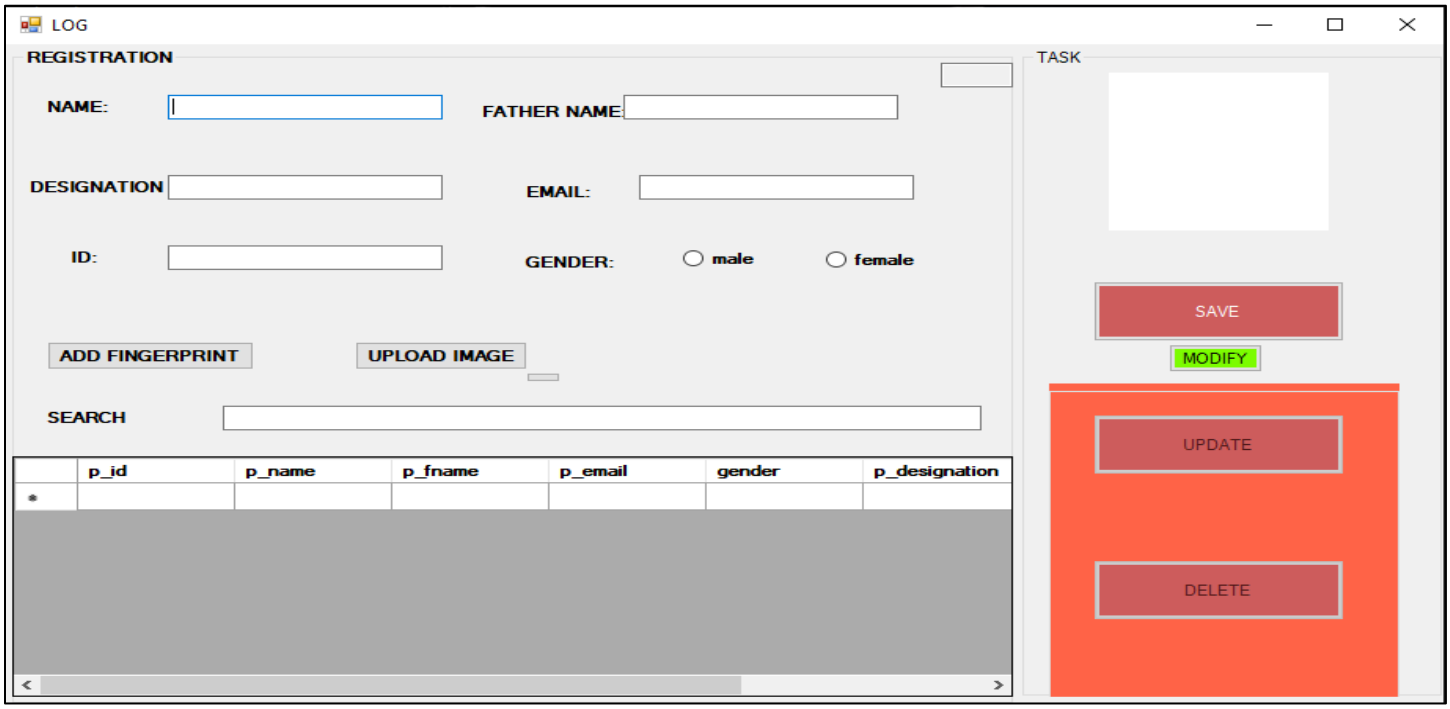

Fig 2: Registration Interface

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR375

D. Fingerprint Scan:

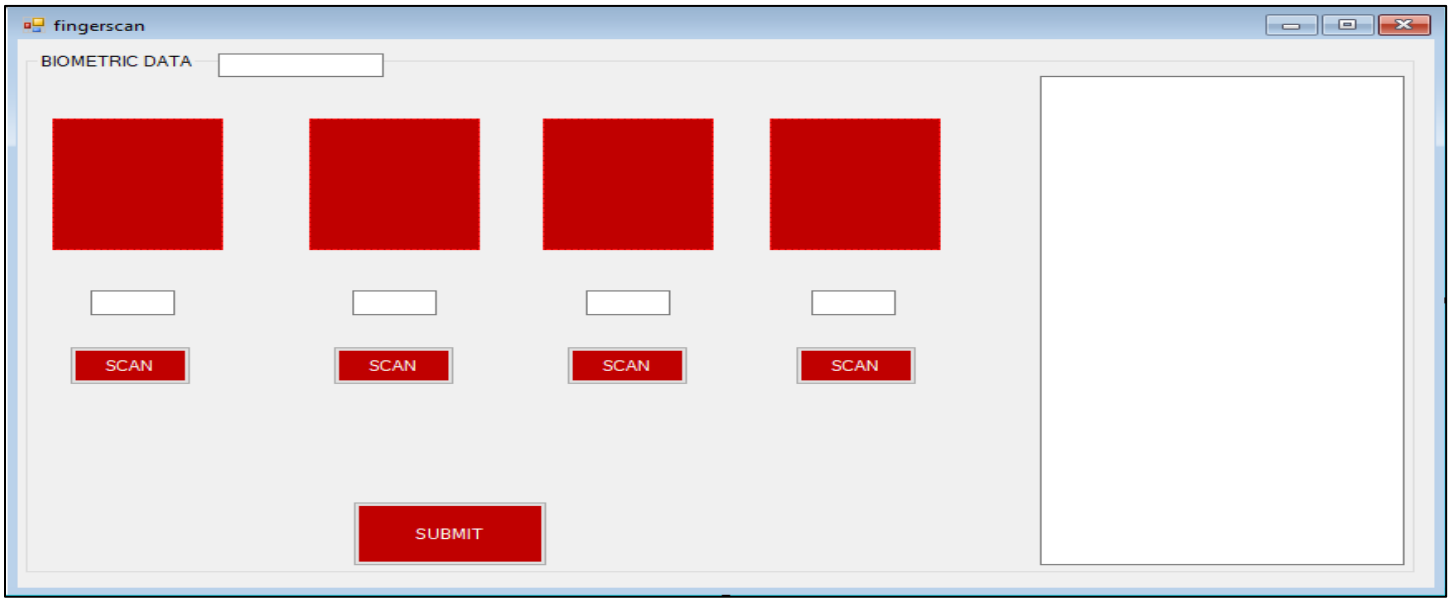

Fig 3: Fingerprint

This fingerprint scan page allows the user to submit four different biometric data points by clicking the scan button. The biometric data is gathered from the registration pages. This page is accessed after the user has registered their basic information. The unique ID they have provided will serve as their biometric data ID. Every biometric piece of information must be submitted by the user. Once the system has accepted it, the information is saved in the database in byte format using the biometrics the user entered. Thus, the administrator can see the data in the database as bytes and the data.

E. Fingerprint Check

Check form used to identify user identity using previously recorded biometric data patterns. Initially, the user fills in each text field with their unique pin for fingerprint data. The fingerprint scanner receives the response from the user when they press the corresponding finger I.D. scan button, allowing it to identify biometric information. If all four biometric entries are successfully reviewed and verified after a sequence of entries, the user can access the submission and proceed with additional processing. The form has an I-D box with the corresponding I-D of the user's details in it. Here, I've used a box to map an attribute to each of the four fingerprints I have in my finger data table.

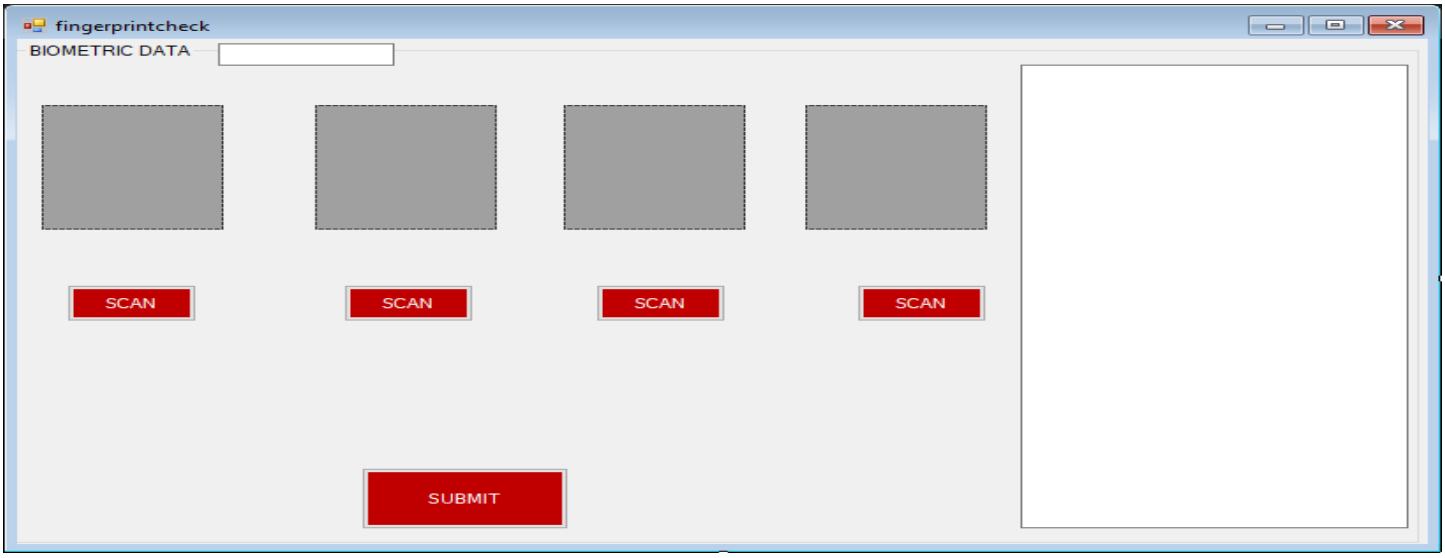

Fig 4: Workflow Diagram

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR375

F. Arduino to Sensor Connectivity

This connection shows that the Arduino board has14 digital inputs/outputs (six of which can be used as PWM outputs), 6 analog inputs, and a 16 MHz ceramic resonator. We have connected a 5 volt sensor to its corresponding Arduino socket, a ground pin from the sensor to the corresponding Arduino Uno ground, a transfer data pin fingerprint to the corresponding Arduino receiving data pin, and a receiving data pin from the sensor to the corresponding Arduino Uno transfer data pin.

VIII. RESULTS AND DISCUSSION

➢ *Future Works:*

- Enhancing the UI and UX design
- Including gestures that make the work of the user easy and convenient.
- Optimizing the data collection much faster.
- In the purpose of automation and the use of machine learning is to predominantly reduce the time complexity even more.
- Surpassing the use of databases by cloud storage because databases might cost large amounts of data.
- Increase in use of this security system in various fields such as home security and many more.
- Enhancement of fingerprint scanner with high FAR (false acceptance rate).
- Development of mobile applications for different use cases.
- Integrating the same methodology with other biometric modalities.

IX. CONCLUSION

In this highly technologically advanced world, even with numerous security mechanisms in place, an individual's data can be transferred via a network relatively readily. However, these security measures all have certain limitations and are susceptible to bias, which can result in data leakage. As a result, we worked together to acquire information on improving data protection and created a multi-pattern fingerprint security system that can act as a firewall for data stored in any type of database. This is the improved, makeshift security system we provide for a single person's privacy.

REFERENCES

[1]. Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles”

[2]. IEICE Transactions on Information and Systems, 2007,90(8):1185-1194.

[3]. Li.W, D. Zhang and Xu.Z, "Palmprint Identification by Fourier Transform," International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 4, pp. 417-432, Jun. 2002.

[4]. Mingxing, HE, HORNG, Shi-Jinn, FAN, Pingzhi, et al. Performance evaluation of score level fusion in multimodal biometric systems. Pattern Recognition, 2010, vol. 43, no 5, p. 1789-1800.

[5]. Meiru Mu, QiuQi Ruan and Yongsheng Shen, "Palmprint Recognition Based on Discriminative Local Binary Patterns Statistic Feature," Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, pp. 193-197, 9-10 Feb. 2010.

[6]. Sanchez-Reillo.R ,Sanchez-Avila.C and Gonzalez-Marcos.A, "Biometric identification through hand geometry measurements," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 22, no. 10, pp. 1168-1171, Oct2000

[7]. Saropourian.B, "A new approach of finger-print recognition based on neuralnetwork," Computer Science and Information Technology, 2009. ICCSIT 2009.2nd IEEE International Conference on, pp. 158- 161, 8-11 Aug. 2009.