IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE BIOGUARD

The Next Generation Security System

[1]Shruti Bhosale, [2]Komal Kachare, [3]Tejas Kini, [4]Reshma Chaudhari

[1]Student, [2]Student, [3]Student, [4]Professor

[1]Department of Computer Engineering,

[1]Mumbai University, Mumbai, India

Abstract: In an era where the need for enhanced security is paramount, the "Secure Bioguard-Next Generation Security System" represents a significant evolution in access control and authentication methods. As the world becomes increasingly interconnected, safeguarding sensitive information, physical spaces, and digital assets has never been more critical. Biometric authentication systems have emerged as a ground breaking solution to address these security challenges. Among these, the integration of multiple fingerprint recognition technologies stands out as a cutting-edge approach to enhancing access control and authentication. This abstract delves into the world of multi-fingerprint security systems, exploring their development, advantages, applications, and the implications they hold for the future of secure access control. The concept of "Secure Bioguard-Next Generation Security System" multi-fingerprint security systems represents a significant leap forward in addressing modern security challenges. By combining the strengths of multiple fingerprint recognition techniques, such as capacitive, optical, and ultrasonic, these systems offer a more robust and versatile approach to authentication.

Keywords- Alternative security in Biometric, Fingerprint Recognition, Multifactor Authentication, Sequence of fingerprints

I. INTRODUCTION

The "Secure Bioguard-Next Generation Security System" as the name suggests, represent a significant evolution in access control and authentication methods. Recently bank security is being a matter of great awareness and importance in the world [1]. In an era where the need for enhanced security is paramount, these systems have garnered attention for their ability to provide a higher level of protection. This synopsis of the “Secure Bioguard-Next Generation Security System” aims to delve into the world of multi-fingerprint security systems, exploring their development, advantages, applications, and the implications they hold for the future of secure access control. In today's digital age, the need for robust security measures has never been more critical. As the world becomes increasingly interconnected, safeguarding sensitive information, physical spaces, and digital assets is paramount. Biometric authentication systems have emerged as a ground-breaking solution to address these security challenges. Among these, the integration of multiple fingerprint recognition technologies stands out as a cutting-edge approach to enhancing access control and authentication. The system “Secure Bioguard-Next Generation Security System” delves into the realm of multi-fingerprint security systems, exploring their evolution, advantages, applications, and implications for the future of security. The concept of “Secure Bioguard-Next Generation Security System” multi-fingerprint security systems represents a significant leap forward in addressing these challenges by combining the strengths of multiple fingerprint recognition techniques, such as capacitive, optical, and ultrasonic, these systems offer a more robust and versatile approach to authentication. This report explores the technical aspects of these techniques, including how they can be integrated to improve security while maintaining user convenience.

II. METHODOLOGY

A proposed IOT module is integrate with desktop application it includes Fingerprint sensor and Arduino UNO to scan the biometrics. The Arduino UNO is the primary controller, for fingerprint matching, the Arduino board is interfaced with the R307 fingerprint sensor. Desktop application contains the credentials such as username, password, email, and capture button for scanning the fingerprint. The fingerprint sensor on the system registers the fingerprints of legitimate users. The fingerprint sensor has saved the fingerprint models of legitimate users after they have been enrolled. It can now check to see if any saved models match fresh scans by comparing them to the current models. Open the serial monitor and upload the fingerprint matching sketch to the Arduino. Users can have enrolled by entering their credentials and registered multiple fingerprints in any sequence. Sequence is stored in the system to extract the pattern to identify each user. If a user wants to login user has to enter their credentials and second phase is system asked for fingerprints, fingerprints in the sequence that entered during registration phase, if patterns and sequence of the fingerprint is matched then user get permit to access the system.

III. COMPONENT USED

3.1 R307 Fingerprint Sensor

A cutting-edge biometric tool for safe and effective fingerprint recognition is the R307 fingerprint sensor. The R307 Fingerprint Module is a comprehensive biometric solution comprising an optical fingerprint sensor, high-speed DSP processor, advanced fingerprint alignment algorithm, high-capacity FLASH chips, and additional hardware and software components. Its stable performance and simple structure facilitate functions such as fingerprint entry, image processing, fingerprint matching, search, and template storage. The module offers independent fingerprint collection, registration, comparison (1:1), and search (1:N) capabilities. Application development is simplified through provided control instructions, enabling developers to create fingerprint-enabled products without extensive expertise in biometrics. In terms of communication protocol, the R307 module supports both UART and USB interfaces, utilizing a common serial communication protocol based on a packet format. All data and commands are transmitted and received as packets, requiring framing of data and commands before transmission and extraction of data from response packets The R307 fingerprint sensor was designed with longevity and dependability in mind, even under harsh climatic circumstances.

3.1 Arduino UNO

Arduino UNO Popular microcontroller board Arduino Uno is a flexible platform for electronic project building and prototyping. The Arduino UNO is a highly popular microcontroller board renowned for its versatility and ease of use, making it an excellent choice for beginners and experienced users alike in the realm of electronics and coding. At its heart lies the ATmega328P microprocessor, running at speeds of up to 16 MHz, providing ample processing power for various tasks. Its rich array of peripherals includes timers/counters, USART for serial communication, SPI and I2C interfaces for communication with other devices, analog comparator, PWM channels for generating analog-like signals, and interrupt capabilities for handling external events. Additionally, features such as Power-On Reset (POR) and Brown Out Detection (BOD) ensure reliable operation, enhancing the board's robustness. It has RX and TX pins for serially communicate between the fingerprint sensors. Powered by a 5V power supply and featuring a USB interface for easy connection to a computer, the Arduino UNO provides a seamless development experience, making it an ideal platform for prototyping, experimentation, and learning in the field of embedded systems and electronics.

IV. REVIEW OF LITERATURE SURVEY

Md. Sumon Sarder, Sujit Kumar Sarkar, et.al[1], Authors has designed a system for bank security is being great awareness and importance among peoples. Though, we designed a multi-layer Bank security system to preserve the bank locker from stealing and unauthorized access [1]. A multi-layer bank locker security system can be legalized, and monitored and prevent security in a bank locker room or unauthorized access. This security system is a highly reliable multi-level security system to protect lockers. This banking security system with a high-security two-door system, multi-layer wall based on infrared radiation and GSM technology, sensors such as sound sensor, motion sensor, laser sensor, gas sensor, IP camera, microcontroller keyboard, LCD monitor, etc.

Dr.Gandhimathi Amirthalingam, Saranya Subramaniam, et.al[2], Authors attempted to synthesize and compare human identification biometric recognition which is the process that determines an individual's identity using physiological or biological traits. Literature reviews of the most recent multimodal biometric

human recognition techniques are presented. Methods that use multiple types of biometric sources for identification purposes (multi-modal biometric) are reviewed. Combination scheme, description and limitation of the biometric sources and database which are used to improve the recognition are given. An evaluation of multi biometric technology and its conclusions are also given in today's fast-paced and interconnected world, ensuring robust security measures is an imperative task.

Arjun Benagatte Channegowda, H N Prakash, et.al[3], The authors provide a unique multimodal biometric recognition model that combines deep learning methods, namely Convolutional Neural Networks (CNNs), with multi-level Histogram of Oriented Gradients (HOG) feature fusion to integrate fingerprints and signatures. In order to maximize classification accuracy, they experiment with different hidden neurons and neural network layers. Using a combination of concatenation and product operations in multilayer feature fusion, they eventually achieved an impressive 93.33% accuracy. Their research highlights the advantages of multimodal biometrics over unimodal systems, especially for bigger datasets, and highlights how deep learning may be used to improve biometric recognition systems.

Alexander Diomidovich Afanasiev, et.al[4], Authors proposed a novel fingerprint identification system integrating image processing and machine learning techniques to enhance processing speed and accuracy, particularly for low-quality fingerprint databases. Their solution consists of feature extraction, database matching, and preprocessing for improving image quality. They get a noteworthy accuracy rate of 97.75% on mixed high- and low-quality fingerprint datasets by integrating morphological approaches with picture segmentation and using artificial neural networks for template matching. In order to solve major issues in contemporary fingerprint recognition, notably in forensic and law enforcement applications, the study makes recommendations for future research areas. These include expanding the system to use deep learning, namely convolutional neural networks, for advanced feature extraction.

Mrs. ASHA K. PATEL, Mrs. Unnati p. Patel, Falguni Suthar, et.al[5], Authors analyze the complexities of biometrics, highlighting its essential function in automated individual identification based on unique biological or behavioral characteristics. Because fingerprint recognition has been used extensively and has a long history of reliability, especially in forensic applications, the authors primarily focus on this technology. They use cutting-edge data mining techniques like neural networks and nearest neighbor algorithms to improve system precision and security as they take on the problem of choosing the best fingerprint matching algorithm to satisfy particular performance and accuracy requirements. They stress that in order to meet targeted performance criteria, it is essential to have a thorough grasp of the architecture of biometric systems and to choose algorithms with care. Their suggested fingerprint identification system, which mostly operates in verification mode, takes advantage of fingerprints' intrinsic uniqueness and dependability, which are well-suited for a wide range of applications.

Sreeramana Aithal, Krishna Prasad Karani, et.al[6], The Authors discusses the significance of fingerprint recognition systems and the crucial role of image enhancement technique with a particular emphasis on Level 1 and Level 2 features. In addition to highlighting the contributions made by different researchers to feature extraction techniques, it emphasizes how crucial it is to improve fingerprint photos in order to increase recognition accuracy—especially in situations where the images are noisy or damaged. In order to achieve high-quality picture identification and automatic matching, the surveyed authors jointly support techniques like wavelet transform, Gabor Filter, Log Gabor filter, Directional filter, Elliptical Gabor filter, Adaptive Filtering, and similar methods. This thorough analysis highlights the continuous efforts made by the scientific community to improve fingerprint recognition systems by utilizing behavioral and physiological traits for reliable and secure identification and verification.

Faiyaz Shahrear, Shamit Nibras, et.al[7], The authors discoursed about an extensive examination of biometric technology as a way to overcome the drawbacks of conventional identification techniques like PINs and passwords. It details the steps involved in fingerprint-based authentication enrollment and verification as well as the general layout of a biometric system. They emphasize how crucial biometric identity systems are to improving security protocols and lowering crime rates. They address the developments and difficulties in fingerprint-based authentication systems, pointing out potential weaknesses, through an extensive analysis of the literature. The study also demonstrates the practical application of an Arduino UNO and Proteus software, demonstrating the viability and effectiveness of a fingerprint-based biometric security system. In general, the

study advances knowledge on how biometric technology might enhance security and access control in a variety of contexts.

Ramses Wanto Tambunan, Abdul Aziz Ar-Rafif, Mia Galina, et.al[8], The authors provide an extensive review of a three-tiered home security system prototype that aims to improve security and give families the ability to monitor their properties remotely. In order to replace conventional door locks with a more effective and safe alternative, the authors want to incorporate fingerprint, RFID, and keypad biometric sensors into the system. They show how effective each sensor is through extensive testing and experimentation; for example, the fingerprint sensor can read fingerprints in an average of 3.7 seconds, the RFID sensor can detect RFID cards in 2.4 seconds, and the keypad sensor can register passwords in an average of 3.66 seconds. An evaluation of the system's overall performance reveals that the 3-level multi-sensor prototype can open doors in an average of 9.78 seconds. The authors' overall goal is to offer a high-security smart home entryway lock solution while putting an emphasis on user control, accessibility, and ease of use.

Jayapandian, Dr.A.M.J.Md. Zubair Rahman, et.al[9], The authors address the security issues that prevent cloud computing from being widely used, placing a strong emphasis on data security and privacy issues. They suggest incorporating fingerprint technology into cloud-based applications as a way to improve security and reduce hazards. The study highlights the necessity for strong security measures by discussing several security challenges that are common in cloud computing, such as data confidentiality, availability, and integrity. To improve authentication procedures and safeguard online transactions, the authors offer a tri-level security architecture that includes biometric authentication, notably fingerprint recognition. A mathematical model for safe cloud data storage is presented, with a focus on the significance of encryption and decryption methods. In conclusion, the article highlights the significance of fingerprint technology in safeguarding online transactions and improving the overall security posture of cloud computing.

N.V. Sai Krishna, Sk Hasane Ahammad, GNS Kumar, et.al[10], In order to solve issues like noise and reinforcement samples in grayscale fingerprint images, the authors of this study describe a CNN-based system for fingerprint authentication and feature extraction. They suggest using FCN layers to extract characteristics directly from the data, with a focus on minutiae extraction—a critical component of fingerprint recognition. By using this method, they hope to improve both the speed and accuracy of fingerprint detection, with a GPU detection speed of 0.45 seconds per fingerprint.

Jayesh Parab, Shruti Kamat, et.al[11], The authors present a fingerprint-based biometric verification system designed to improve security in a variety of environments, including homes, offices, retail stores, and industrial facilities. They emphasize the benefits of fingerprints as a biometric verification method because of their uniqueness. In particular, they suggest a system that uses fingerprints instead of actual keys for lockers, reducing security risks associated with unwanted entry. To improve security monitoring and capture user data, the system incorporates an IoT platform. They also talk about how the project might be used in offices to track facility usage and make sure only authorized people have safe access. The authors want to address security issues and offer a dependable biometric authentication solution through their work.

Falmata Modu, Audu Mabu et.al[12], provided a study on biometric-based authentication systems, is introduced in the abstract, along with some of the difficulties they encounter, like spoofing attempts and mistakes brought on by noisy data. It suggests merging a decision-level multibiometric system with a trust management system to increase accuracy and lower energy consumption. The efficiency of the suggested system was tested by the authors through experiments, and they discovered significant improvements in the reduction of false positive rates and energy usage. An extensive description of the suggested system, including its execution and evaluation outcomes, is given in the paper. The paper ends with recommendations for further research, including investigating ideal parameter values with the use of meta-heuristic methods.

Navdeep Kumar, R.K. Rowe, et.al[13], The progression of security mechanisms, from conventional passwords and PINs to biometric systems that authenticate people based on their physiological and behavioral traits, is covered in the paper. It highlights the benefits of multi-modal biometric systems over uni-modal ones in terms of security and recognition rates. It is stressed how crucial biometric authentication is in a number of industries, such as transportation and healthcare. Both the identification and verification procedures are included in the explanation of the architecture and operation of biometric authentication systems. The conclusion emphasizes how important biometric technology is to improving security measures around the

world, particularly in light of emerging dangers like terrorism. It implies that multi-modal biometric systems are more accurate than uni-modal ones, giving researchers and practitioners in biometrics an extensive overview of the field.

Riya Deshmukh, Sharad Mohod, et.al[14], The authors discuss the value of biometric systems in several domains as well as the difficulties they encounter, namely with relation to biometric data collection and spoofing assaults. They present a novel solution to these problems by combining biometric information from fingerprints and palmprints with a random forest classifier to improve security and thwart spoofing attacks. Using machine learning techniques and multi-modal biometric data, the scientists hope to improve the security of biometric systems and stop spoofing attempts.

Zurida Ishak, Narmitha Rajendran, et.al[15], The authors introduce a biometric system focusing on fingerprint recognition for identity authentication, particularly in high-security environments using encryption techniques and multifactor authentication techniques, this suggested system seeks to improve security. Administrators can restrict user access permissions and keep an eye on system activities thanks to the Biometric Fingerprint Sensor that is linked to a central system. To stop unwanted access and data leaks, the system applies position-based access control and updates data changes on a regular basis. The main objective is to solve issues like illegal access and lax security enforcement by offering an easy-to-use and practical solution for protecting sensitive data in businesses.

V. ANALYSIS TABLE

Table 5.1: Analysis Table

Title	Summary	Advantages	Technique
Multi Level Bank Locker Security System with Digital Signature Authentication and Internet of Things. (2022) [1]	A Multi-Level Bank Locker Security System with Digital Signature Authentication and Internet of Things is a cutting-edge solution designed to enhance the security of bank lockers and provide convenient access control for customers.	Instant Alerts: The system can send instant notification. Real-Time Monitoring: IoT integration allows for real-time monitoring of locker access.	Digital signature algorithms (e.g., RSA, DSA, ECDSA)
Multi Modal Biometric System: A Review on Recognition Method.(2017) [2]	A Multi-Modal Biometric System is a comprehensive security solution that combines multiple biometric recognition methods to enhance accuracy and security.	Enhanced Accuracy: Combining multiple biometric modalities increases authentication accuracy by reducing the likelihood of false positives and negatives.	Algorithms: Eigen faces, Fisher faces, Local Binary Patterns (LBP), and Deep Learning-based models (Convolutional Neural Networks - CNNs).

Multimodal biometrics of fingerprint and signature recognition using multi-level feature fusion and deep learning techniques.(2021) [3]	Multimodal biometrics involving fingerprint and signature recognition employs advanced techniques like multi-level feature fusion and deep learning. Achieved an impressive 93.33% accuracy.	Higher Confidence Levels: The fusion of features at different levels adds layers of confidence to the authentication process, making it more reliable for critical applications.	Multi-Level Feature Fusion, Privacy-Preserving Techniques.
Automatic Identification Fingerprint Based on Machine Learning Method(2021) [4]	Automatic identification based on fingerprint recognition using ML methods involves utilizing ML algorithms to develop systems that improving image quality and segmentation to identify the fingerprint area, extracting features, and matching the database.	High Accuracy: Machine learning models can achieve high accuracy in fingerprint recognition, reducing the chances of false positives and false negatives.	Machine Learning Algorithm (SVM, k-NN), Deep Learning(CNNs, RNNs, RNNs).
Recognition in Biometric Security System.(2021)[5]	Recognition in biometric security systems involves the process of identifying or verifying individuals based on their unique physiological or behavioral traits.	High reliability & Scalability: Biometric systems can be easily scaled to accommodate a large number of users.	Biometric Modalities, Matching Algorithms
Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. (2017) [6]	The biometric feature most frequently used for identification and verification. Macro details found in Level 1. But when combined with level 2 or level 3 features, these strengthen and secure the fingerprint recognition system.	Goodness Index, Gabor Filter Fast fingerprint enhancing algorithm. Local ridge orientation and ridge frequency which improves the performance of the matching process.	Image Enhancement Techniques, Pre-processing and Image Acquisition

Fingerprint based biometric security system Microprocessor and Embedded System. (2021) [7]	In biometrics can be used to determine and identify of any unknown person in two ways. Verification and identity, in other words. In forensic applications, criminal investigations, terrorist identification, and other security purposes, fingerprint verifications play a critical role.	Minimal User Training: Users do not require extensive training those fingerprint-based systems, simplifying adoption.	Fingerprint Sensor Technology, Microprocessor and Embedded System Hardware.
Multi-Security System Based on RFID Fingerprint and Keypad to Access the Door. (2022)[8]	The System based on fingerprint recognition, and a keypad is a sophisticated door access control system.	Customization: It can be customized to fit various access control scenarios, making it suitable for both residential and commercial applications.	RFID Technology, Fingerprint Recognition Technology, Microcontroller or Microprocessor.
A Novel Approach to Enhance Multi Level Security System Using Encryption with Fingerprint in Cloud. (2016)[9]	Cloud computing has transformed the economics of IT by lowering costs for both providers and users. It offers efficient resource provisioning and widespread adoption.	Strengthens security through cloud-based fingerprint encryption for robust authentication.	Cloud Computing Technology, Multi-Factor Authentication (MFA).
Security Systems for Identification and Detection Fingerprint Based On Cnn and Fcn. (2020) [10]	The Characteristic extraction is an essential biometric authentication phase and recognition systems. In this paper a CNN's based algorithm for Fingerprint Authentication and Feature Extraction has been presented.	Robust Feature Extraction: CNNs can automatically learn and extract relevant features from fingerprint images, CNN and FCN-based models typically require minimal maintenance and cost in long-period.	Real-Time Processing, Cross-Validation and Evaluation Metrics, Fully Convolutional Networks (FCN).
IoT Based Smart Biometric Locker.(2022)[11]	Advanced locking system techniques are replacing the conventional mechanical lock and key mechanisms. These methods combine mechanical and electronic devices in highly intelligent ways.	Enhanced security through biometric authentication and remote monitoring capabilities.	Internet of Things (IoT) Technology, Mobile Applications

Multibiometric System for Internet of Things using Trust Management. (2020) [12]	In this paper, a trust management system is used together with a decision level multi-biometric system to improve the accuracy and lower the energy consumption of the proposed system.	Trust management systems allow for dynamic adjustments in access privileges and trust levels based on user or device behavior.	Trust Management Technologies, Human-Computer Interaction (HCI),Machine Learning and Data Analytics.
A Study of Biometric Identification and Verification System (2021) [13]	A distinct and quantifiable characteristic used to identify and characterize a person is called a biometric identifier. Considering that a multi-model biometric system offers greater accuracy than a single-model system.	Accuracy and Reliability: Biometric systems offer high accuracy and reliability in identifying individuals, as they are based on unique physiological or behavioral traits that are difficult to forge or manipulate.	There are various available methods for identification such as Face Recognition, Iris Recognition, Voice Recognition, Fingerprint Recognition
Biometric Jammer: A Prevention of Fake Acquisition of Fingerprint for security Enhancement. (2022) [14]	Biometrics is an effective security technique that can be used in a variety of contexts, including law enforcement, civilian applications, mobile device security, and military use. Despite the fact that the biometric system must deal with the most frequent issues, such as spoofing attacks and the collection of biometric data.	Integrating multiple biometric modalities adds layers of security, making it more difficult for unauthorized users to gain access.	Technologies used in these jammers can vary, but they often involve radio frequency (RF) jamming to disrupt communication between the biometric sensor and the system that communicates with it.
Secure Biometric Lock System for Files and Applications: A Review (2020) [15]	As a result of modern technological advances, biometric authentication is being used in increasingly more securely secured companies. The primary widely used mass market application of a biometric verification element is unique finger impression identification.	Biometric locks offer a higher level of security since biometric data is unique and difficult to copy exactly.	The paper reviews a secure biometric lock system for files and applications, employing technologies like fingerprint recognition, AES encryption, and access control mechanisms such as RBAC and MFA

V. RESULTS AND DISCUSSION

5.1 Block Diagram

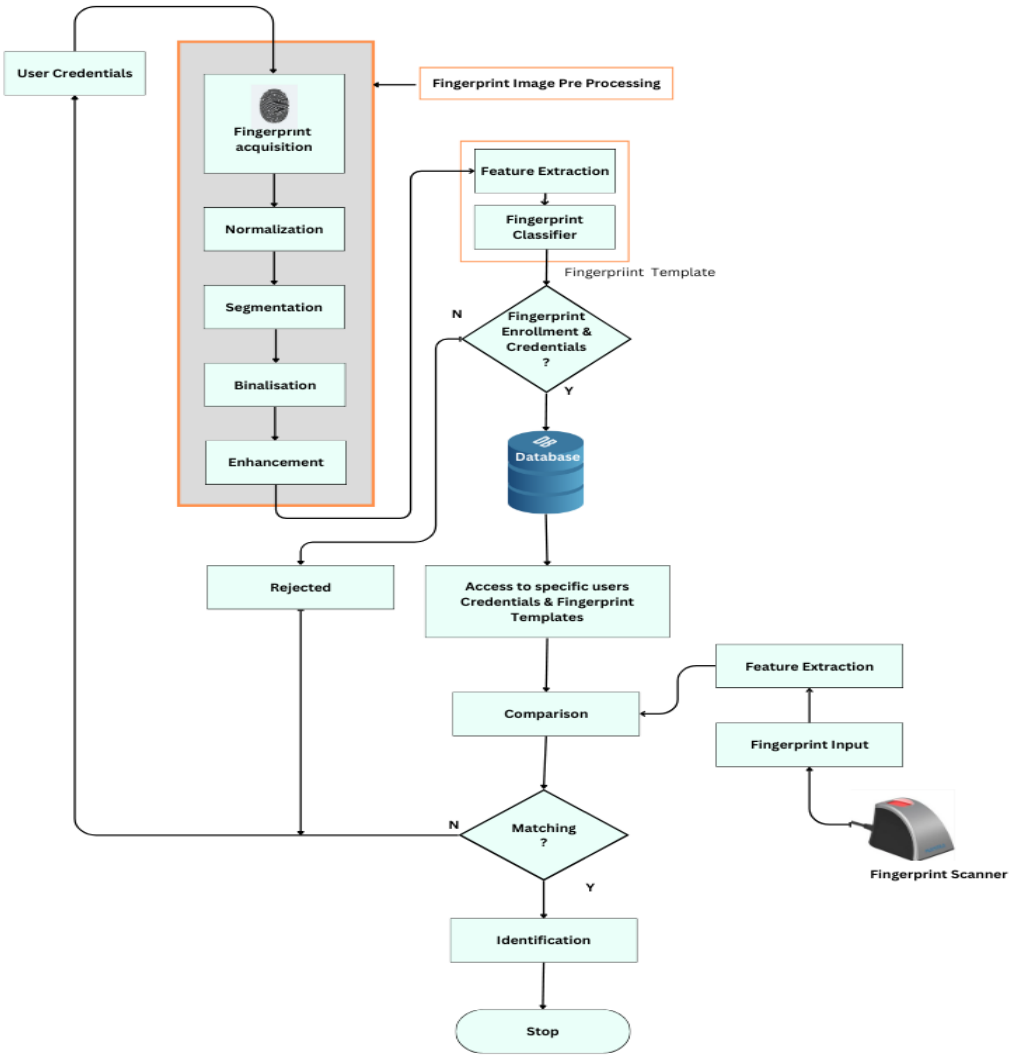

Fig 5.1 Block Diagram

Figure 5.1 Shows the General Flow of the proposed system in which the principal parts and functions are represented by blocks which are connected by lines that show the relationships of the said blocks.

5.2 Implementation Results

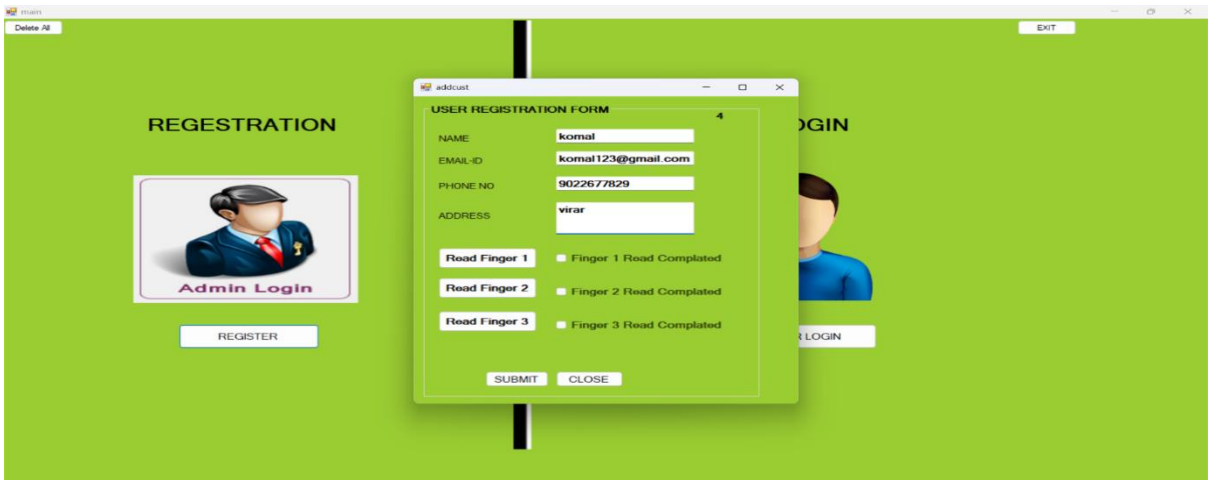

Fig 5.2 Register Window of Secure BioGuard

Figure 5.2 show the Register window of system, user can register by using basic credentials such as name, email id, phone etc. and the second phase is the to register fingerprints.

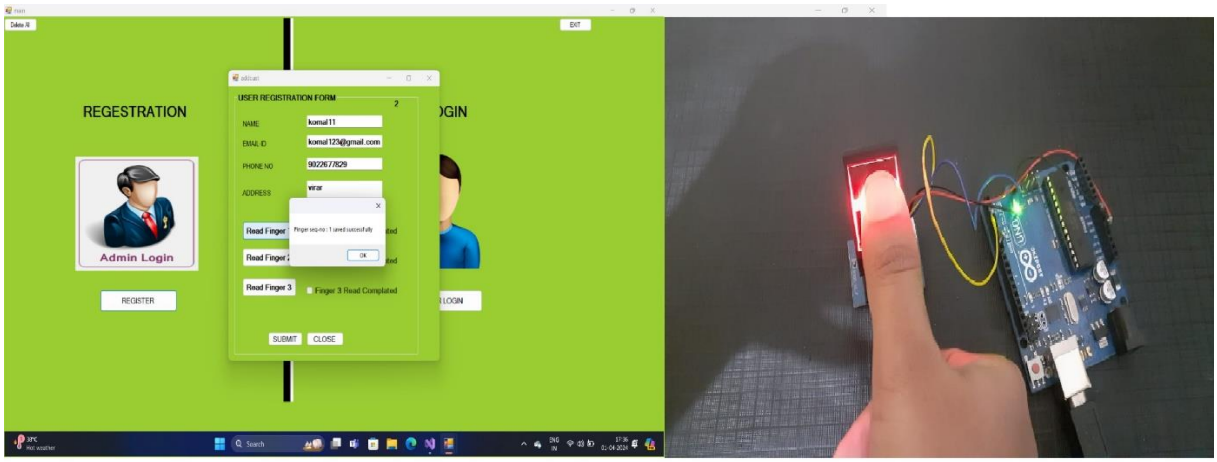

Fig 5.3 Register Fingerprints in Sequence

Figure 5.3 shows user should have to scan fingers on the fingerprint module and they can use multiple fingers but in the sequence, user can use any sequence and the registration is done successfully.

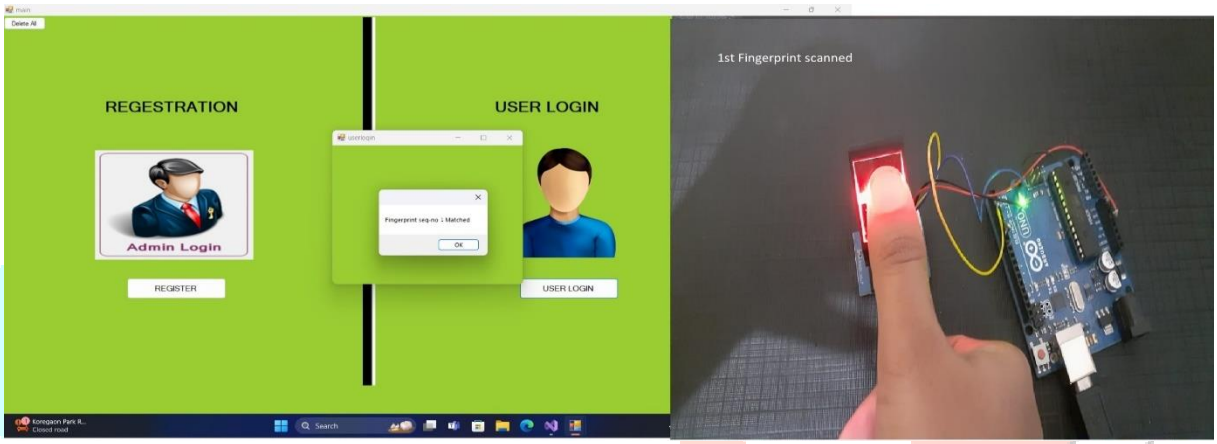

Fig 5.4 Login

Figure 5.4 shows, when user have to access the system, user must provide the traditional login credentials in the first layer and in the second layer ask to fingerprints in the sequence if sequence is matched then user can access the system otherwise user is blocked.

Fig 5.5 Home Screen of Secure BioGuard

Figure 5.5 shows, when user successfully scanned all the fingerprints in the sequence then system will have authorized user to access the system and home screen will have displayed.

VI. FUTURE SCOPE

Further research in the "Secure Biogurad-Next Generation Security System" could focus on exploring alternative biometric authentication methods such as incorporating blockchain technology to safeguard user credentials and access logs, which could offer impenetrable security. Adaptive security measures and privacy-preserving measures have the ability to dynamically modify security procedures in response to a range of parameters, including threat levels, environmental conditions, and user behavior. It protects against future issues, and maintaining the privacy of your information and ensuring that it functions properly with other systems are also crucial.

VII. CONCLUSION

Secure BioGuard Next-Generation Multi Fingerprint System is a state-of-the-art biometric security system that uses multiple fingerprints to identify individuals with high accuracy and security. It is used in a variety of high-security applications, including access control, law enforcement, and border security. The SBNGFS is resistant to a variety of attacks. Users can quickly and easily authenticate themselves using their enrolled fingerprints, making it a convenient choice for security personnel and individuals alike. Its multi-fingerprint approach, resistance to attacks, and adaptability make it a valuable asset for organizations and agencies that demand the utmost in security and accuracy.

REFERENCES

[1] Md. Ashiqul Islam, Md. Sumon Sarder “Multi Level Bank Locker Security System with Digital Signature Authentication and Internet of Things”,*Research Square*, 2022.

[2] Dr.Gandhimathi Amirthalingam, Saranya Subramaniam, “Multi Modal Biometric System: A Review on Recognition Method”, *International Journal of Engineering Research & Technology(IJERT)*, 2017.

[3] Arjun Benagatte Channegowda1, H N Prakash “Multimodal biometrics of fingerprint and signature recognition using multi-level feature fusion and deep learning techniques”, *Indonesian Journal of Electrical Engineering and Computer Science Vol. 22, No. 1, April 2021*.

[4] Long The Nguyen, Huong Thu Nguyen, Alexander Diomidovich Afanasiev, Tao Van Nguyen,“Automatic Identification Fingerprint Based on Machine Learning Method”, *Journal of the Operations Research Society of China*, 2021

[5] Mrs ASHA K. PATEL, Mrs. Unnati p. Patel, Falguni Suthar, “Fingerprint Recognition in Biometric Security Systems", *Research Gate*, May,2021.

[6] Sreeramana Aithal Krishna Prasad karani “Literature Review on FingerprintLevel 1 and Level 2 Features Enhancement to improve Quality of Image”, *International Journal of Management, Technology, and Social Sciences (IJMTS)*, July,2017.

[7] Faiyaz Shahrer, Huzaifa Abdulla AI Azad , Mustasim Mahmud, Shamit Nibras, “Fingerprint based Biometric Security Microprosessor and Embedded System”, *Research Gate*, 2021

[8] Ramses Wanto Tambunan , Abdul Aziz Ar-Rafif , and Mia Galina “Multi-Security System Based on RFID Fingerprint and Keypad to Access the Door”, *Jurnal Teknik Elektro, Vol. 14, No.2*, October, 2022.

[9] M.Koushikaa, S.RadhikadeviA , “Novel Approach to Enhance Multi Level Security System Using Encryption with Fingerprint in Cloud”, *Institute of Electrical and Electronics Engineers(IEEE)*, 2016

[10] N.V.sai Krishna ,Sk Hasane Ahammad,GNS Kumar, “Security system For Identification And Detection Fingerprint based on CNN And fcn”, *Institute of Electrical and Electronics Engineers(IEEE)*, 2020.

[11] Jayesh Parab, Shruti Kamat, “IoT Based Smart Biometric Locker”, Social Science Research Netword (SSRN), 2022.

[12] Falmata Modu,Yusuf Sani, “Multibiometric System for Internet of Things using Trust Management”, *Institute of Electrical and Electronics Engineers(IEEE)*, November, 2020

[13] Navdeep Kumar, R.K. Rowe, “A study of Biometric Identification and Verification System”, *Institute of Electrical and Electronics Engineers(IEEE)*, June, 2021.

[14] Riya Deshmukh, Sharad Mohod, “Biometric Jammer: A prevention of Fake Acquisition of Fingerprint for Security Enhancement”, *Institute of Electrical and Electronics Engineers(IEEE)*, June, 2021.

[15] Zurida Ishak, Narmitha Rajendran, “Secure Biometric Lock System for Files and Applications: A Review”, *Institute of Electrical and Electronics Engineers(IEEE)*, 2020