SMART DOCUMENT PROTECTION SYSTEM WITH DUAL BIOMETRIC AUTHENTICATION AND SECURITY ALERTS

Bodatati Sesirekha [1],Dr. G. Srinivasa Rao[2], Gogula Pavani [3], Munaga Aswitha [4], Matcha Rajani [5]

*Bodatati Sesirekha[1] Department of Electronics and Communication Engineering,
Bapatla Women's Engineering College
Dr. G. Srinivasa Rao[2] Department of Electronics and Communication Engineering,
Bapatla Women's Engineering College
Gogula Pavani [3] Department of Electronics and Communication Engineering,
Bapatla Women's Engineering College
Munaga Aswitha [4] Department of Electronics and Communication Engineering,
Bapatla Women's Engineering College
Matcha Rajani [5] Department of Electronics and Communication Engineering,
Bapatla Women's Engineering College*

---***---

Abstract - In today's digital landscape, the protection of sensitive and confidential documents has become critically important to prevent unauthorized access and potential data breaches. This project presents a Smart Document Protection System that leverages dual biometric authentication and IoT-enabled security alert mechanisms, ensuring a secure and intelligent approach to document protection. The core of the system is built around an Arduino Uno which manages the hardware-side authentication processes. The security system implements a two-step fingerprint authentication and a secure password check, allowing only verified users to gain access to the protected documents. Upon successful biometric and password verification, the system automatically unlocks an electronic door lock, granting access to the stored documents. In the case of an incorrect password or unauthorized access attempt, the system triggers a Python-based script to capture an image using the laptop's camera and sends a real-time alert with the photo to the concerned authority via Telegram messaging SMS notification.

Key Words: Arduino Ide Software, Telegram API, Arduino C language, Real-time Security Alerts.

1.INTRODUCTION

In today's digital era, the protection of sensitive physical documents remains a critical challenge, especially in environments like government offices, corporate sectors, and personal safes. Traditional security measures such as key locks or single-factor authentication systems are often insufficient, as they can be easily bypassed or compromised.[2] To overcome these limitations, this project introduces a Smart Document Protection System that uses a multi-layered authentication approach for enhanced security. The system is built using Arduino Uno for managing hardware operations and Python for software-based tasks like surveillance and alerts. It includes dual biometric fingerprint scanning followed by a password check, ensuring that only authorized users can access the documents. Upon successful verification, a servo motor unlocks the secured compartment. In the event of a failed authentication especially due a wrong password a Python script is triggered to capture the intruder's image using a webcam and sends a real-time alert via Telegram and SMS to the concerned authority. This integration of biometric, password, and IoT-based alert systems offers a reliable, efficient, and cost-effective solution for document protection. The system provides both preventive and responsive security, making it suitable for critical use in high-security applications. The principal weakness of these systems is that identification cards may be lost or stolen, and secret codes may be stolen, guessed or determined by trial and error. There has been a trend toward systems that avert the need to carry identification cards or to memorise secret codes.

2. LITERATURE REVIEW

[1] Yuhanim Hani Binti Yahaya -The paper titled "Fingerprint Biometrics Authentication on Smart Card" explores the integration of fingerprint recognition technology with smart cards to enhance user authentication and identification systems. It addresses the limitations of traditional authentication methods—such as passwords and physical cards—by leveraging the uniqueness and reliability of biometric data, particularly fingerprints.

[2] Dinesh Bhatia, Anu - In International Journal of Medical Engineering and Informatics, Anu and Bhatia proposed a smart door access system utilizing a fingerprint biometric module for enhanced security. The system employs both hardware and software integration, including a fingerprint sensor (R305), ATmega328 microcontroller, and emergency alert mechanisms. It aims to allow access only to authorized users and is suitable for high-security environments such as ICUs, defence offices, and labs.

[3] Ravi Shekhar Tiwari, Tapan Kumar Das - In the 2024 IEEE 5th International Conference on Circuits, Control, Communication and Computing (I4C), the authors introduced a smart locking system based on multimodal biometrics authentication integrating fingerprint recognition, facial recognition using the SSD algorithm, and RFID verification. The system enhances security by requiring multiple biometric verifications and provides feedback using red and green lights for authentication results.

[4] In Nigerian Journal of Technological Development, the authors presented a prototype model of an IoT-based door system using double-access fingerprint authentication. The model integrates fingerprint sensors, Arduino microcontroller with Ethernet shield, relay modules, solenoid locks, and a web

server to enhance hotel room security. Fingerprints are captured during booking and at the door, with access granted only when both matches. The system achieves 95% success rate under normal conditions and provides an improved, reliable alternative to traditional single-authentication methods.

[5]Elavarasi K and Mohana V-In Smart Fingerprint Authentication and Alert System Using IoT, the authors proposed a fingerprint-based smart door locking mechanism integrated with IoT technology. The system uses an Arduino UNO and fingerprint module to authenticate users, with OTP verification and alert mechanisms using Twilio SMS API to ensure enhanced security and access control.

[6] Mohammed Alaa Yousif Ali, Ehab AbdulRazzaq Hussein -In the proceedings of the 2nd AL Muthanna International Conference on Engineering Science and Technology (MICST-2022), the authors proposed a multi-security system based on a fingerprint biometric sensor and a Wi-Fi camera. The system utilizes an Arduino microcontroller integrated with a local server for real-time authentication and monitoring.

[7] K.S. Tamilselvan, G. Murugesan - This paper addresses the issue of two-wheeler theft by proposing a cost-effective biometric-based security system. The primary innovation lies in using a fingerprint scanner integrated with an Arduino microcontroller to authenticate users before starting the vehicle.

[8] C. Thirumarai Selvi, Surabhi P.S - This paper proposes a smart system that enhances traffic management and document authentication using RFID and fingerprint modules. The system utilizes IoT, Raspberry Pi, MySQL, and PHP to automate license verification and vehicle tracking. It allows traffic authorities to access vehicle and license data instantly, minimizing corruption, paperwork, and manual checks, thereby improving efficiency and promoting a more digitalized infrastructure for law enforcement.

[9] Arvind R Ghosh, Meghna R Raheja - This paper introduces an innovative anti-theft security system that combines IoT, biometric fingerprint authentication, and email-based alert mechanisms to enhance home and office safety. The proposed system is compact and user-friendly, capable of capturing intruder images and sending them via email when unauthorized access attempts occur.

[10] Meenakshi N, Monish M - This paper introduces an Arduino-based smart fingerprint authentication system aimed at enhancing home and office security through a three-level protection method. The system incorporates fingerprint recognition, image-based passwords, and one-time passwords (OTPs) sent via GSM.

3.EXISTING SYSTEM

In most traditional setups, document protection is limited to manual locking mechanisms such as key-based locks, PIN entry systems, or single-layer electronic access using RFID cards or fingerprint scanners. These systems often rely on single-factor authentication, which is susceptible to breaches if the key is lost, the password is guessed, or the biometric sensor is bypassed. There have been some circumstances that can be quite frustrating, such as when a person accidentally locks themselves out of their home or place of business, when they forget their key inside, or when a criminal just busts the lock and makes off with everything within[1]. Additionally, existing security systems typically lack real-time alert capabilities. If an unauthorized access attempt occurs, there is no automated method to inform the concerned individuals immediately. Moreover, most systems are standalone, meaning they don’t integrate with smart devices or communication networks to enhance surveillance and monitoring.

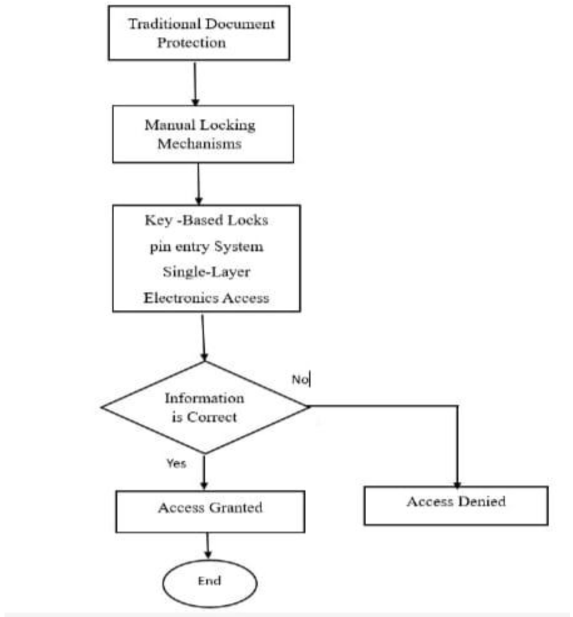

Fig-1: Block Diagram

4.PROPOSED SYSTEM

The proposed system overcomes these limitations by introducing a multi-layered smart security solution that uses dual biometric fingerprint authentication combined with secure password verification for robust document protection. Unlike conventional systems, the proposed solution requires two successful fingerprint verifications from the user before accepting a password, making unauthorized access extremely difficult. In case of a failed attempt particularly due to a wrong password after biometric verification the system uses a Python script to activate the laptop camera, capture the intruder’s image, and send a real-time alert to a registered Telegram account along with an SMS notification to the concerned person. This smart integration ensures that unauthorized access attempts are immediately reported with evidence. The locking mechanism is controlled via Arduino Uno, which interfaces with fingerprint modules and servo motors, providing a cost-effective and reliable hardware platform. Python handles software-side operations, such as camera control and internet-based communication, reducing manual setup issues and increasing automation. This dual-platform integration (Arduino + Python) transforms a basic security system into a smart, IoT-enabled document protection solution suitable for critical applications in government agencies, corporations, research institutions, and personal safes. With enhanced authentication, automated surveillance, and immediate alerts, the proposed system ensures a much higher level of document security than existing methods.

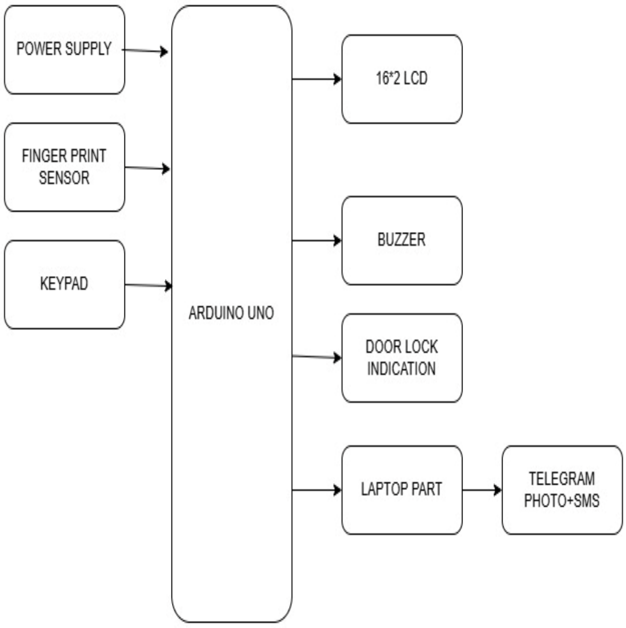

Fig-2: Block Diagram

5. MODULES DESCRIPTION

5.1 Arduino Uno

The Arduino Uno is an open-source microcontroller board based on the ATmega328P. It is designed to make digital electronics easy to use for beginners and professionals alike. The board features 14 digital input/output pins, 6 analog inputs, a USB connection for programming, and is powered by a 5V supply.

Fig-3: Arduino Uno

5.2 Power Supply

Power supply provides electrical energy to a circuit or device by converting and regulating voltage from a source. It can be AC or DC and is essential for the proper functioning of electronic components.

Fig-4: Power Supply

5.3 Fingerprint Sensor

A fingerprint sensor is a biometric device used to capture and recognize a person's unique fingerprint pattern. It plays a crucial role in identity verification an access control system, offering a secure and convenient method of authentication.

Fig-5: Fingerprint Sensor

5.4 16*2 LCD

A 16x2 LCD is a character display module that can show 2 lines of 16 characters each. It's one of the most used display modules in embedded systems for displaying simple text. embedded systems for

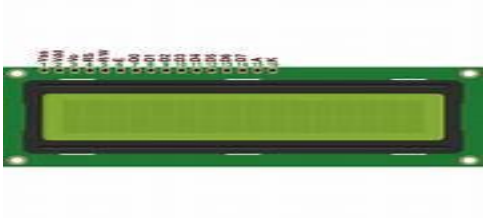

Fig-6:16*2 LCD

5.5 Keypad

A keypad is an input device arranged in a matrix of rows and columns used to enter numeric or alphanumeric data. It's commonly used in embedded systems for tasks like password entry.

Fig-7: Keypad

5.6 Buzzer

A buzzer is an audio signaling device that produces sound when voltage is applied, commonly used for alerts or notifications.

Fig-8: Buzzer

5.7 Servo motor

A servo motor is an electromechanical device that allows precise control of angular position. It consists of a motor, a feedback sensor, and a control circuit**.**

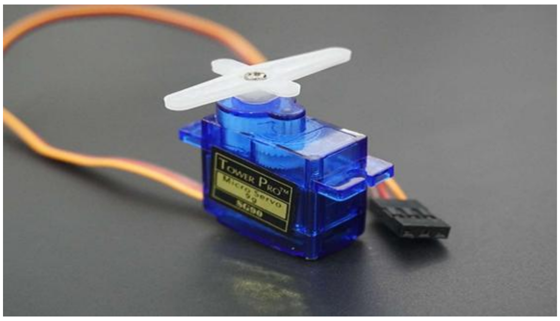

Fig-9: Servo Motor

6.Working Process

The proposed Smart Document Protection System works by combining fingerprint authentication, password verification, and real-time alerts to ensure secure access to confidential documents. The process starts when a user scans their fingerprint using a sensor connected to the Arduino Uno. The system requires two valid fingerprint scans for added security. Once both scans are verified, the user is then prompted to enter a password. If the password is correct, the Arduino activates a servo motor to unlock the document storage area. However, if the password is incorrect, a Python script on a connected laptop automatically captures an image using the webcam and sends an alert message along with the photo to a registered Telegram account and as an SMS to the concerned person. This ensures that any unauthorized access attempt is immediately recorded and reported. By combining hardware authentication with smart software-based alerting, the system offers a secure and intelligent solution for document protection**.**

Flow Chart

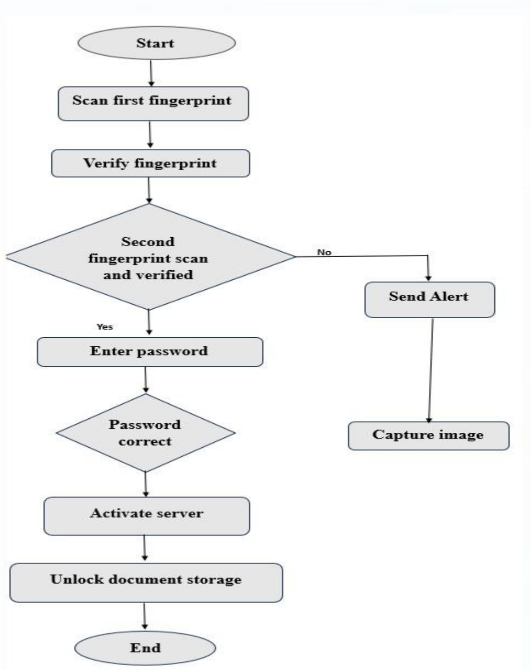

Fig-10: Flow Chart

7.Results

The figure below shows the smart document protection with dual biometric authentication and security alerts. At first we to have place 1st finger and verify it and then place 2nd finger and enter password ,if information is correct access granted. If it does not, it captures the image and sends it to Telegram.

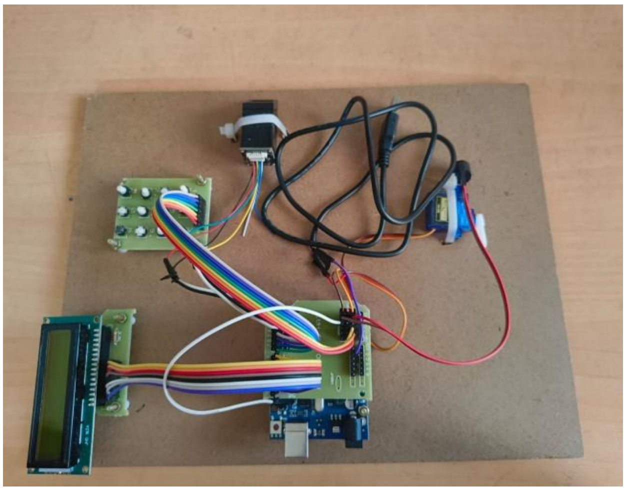

Fig-11: Circuit

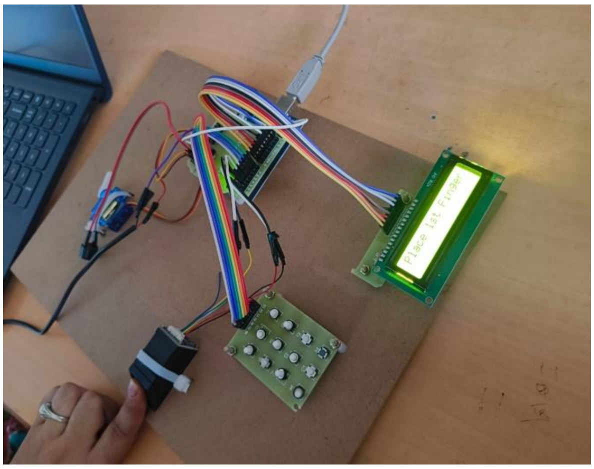

Fig-12: Place 1st Finger

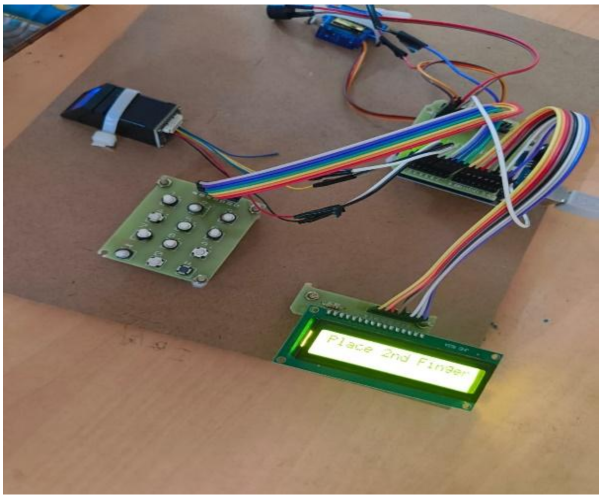

Fig-13: Place 2nd Finger

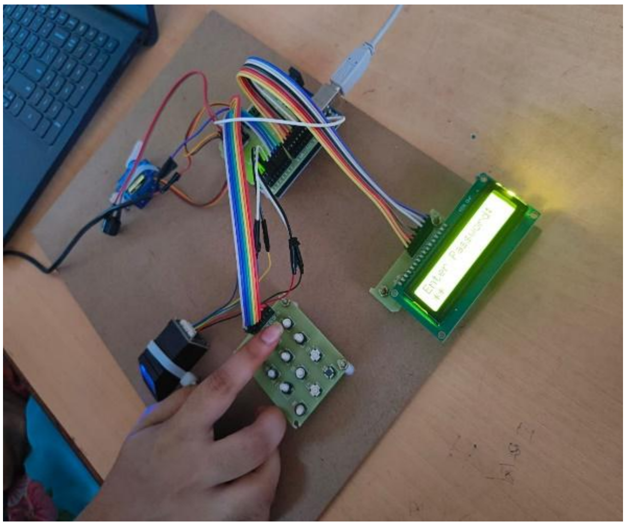

Fig-14: Enter Password

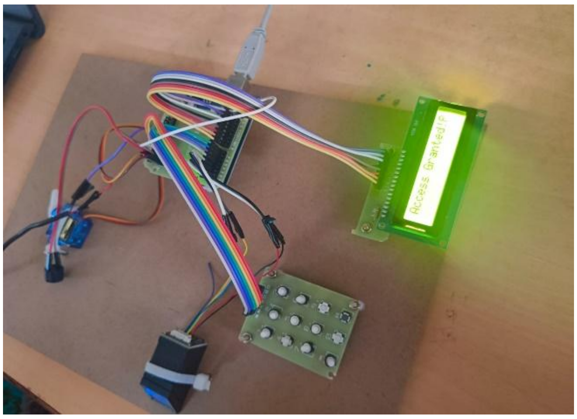

Fig-15: Access Granted

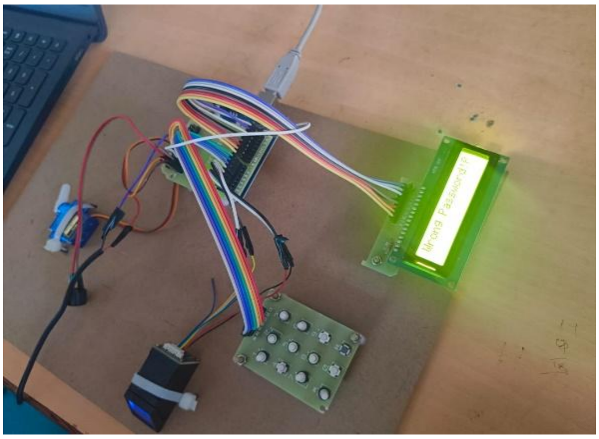

FIG-16: Wrong Password

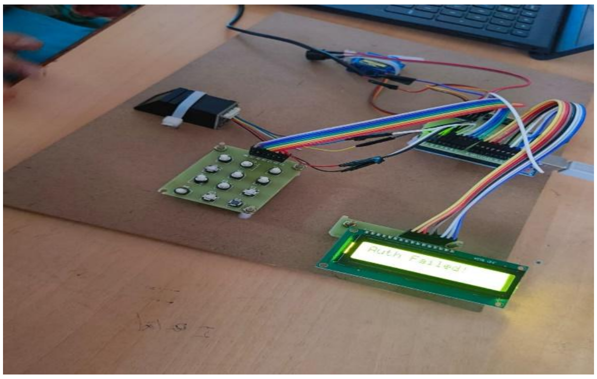

FIG-17: Authentication Fail

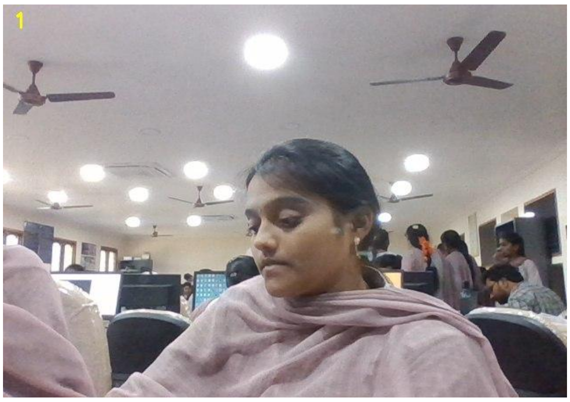

Fig-18: Capture Image

8. COMPARISON

Feature	Existing System	Proposed System
Authentication	Single-factor (key, PIN, RFID, or fingerprint)	Dual fingerprint + password
Security Layers	Basic authentication, easily compromised	Multi layer authetication (biometric + password)
Alert Mechanism	Generally absent or manual	Automated alerts via Telegram and SMS with captured image
Surveillance	No surveillance or manual	Camera-based evidence capturing during unauthorized attempts
Integration with IoT	Limited or none	Integrated with Python, Arduino, and IoT Systems

9. CONCLUSION

The Smart Document Protection System developed in this project successfully demonstrates a secure and intelligent solution for safeguarding physical documents using dual biometric authentication, password verification, and real-time alert mechanisms. By integrating fingerprint sensors with Arduino and combining it with Python-based automation for capturing images and sending alerts via Telegram and SMS, the system ensures multi-layered security. The dual fingerprint scans followed by password entry significantly reduce the chances of unauthorized access, while the instant alert system provides real-time monitoring and quick response to intrusion attempts. The use of low-cost components and open-source platforms makes the system affordable and adaptable for a wide range of applications, from personal safes to sensitive government document protection. Overall, this project achieves its goal of enhancing document security using IoT and biometric technologies in an efficient and reliable manner.

10.FUTURE SCOPE

In the future, the system can be enhanced further by integrating additional features such as facial recognition, voice authentication, or RFID-based access for multi-factor authentication.

REFERENCES

[1] Elavarasi K and Mohana V. “Smart Fingerprint Authentication and Alert System Using IoT.” In: *Proceedings of the 2nd International Conference on Smart Technologies and Systems for Next* Generation Computing (ICSTSN) (2023). IEEE. DOI: 10.1109/ICSTSN57873. 2023. 10151621 .Accessed via IEEE Xplore on February 21, 2025.

[2] Anu and Dinesh Bhatia. “A Smart Door Access System Using Fingerprint Biometric System.” In: *International Journal of Medical Engineering and Informatics* 6.3 (2014), pp.274–280.URL: https://www.researchgate.net/publication/264836924.

[3] Yuhanim Hani Binti Yahaya, Mohd Rizal Bin Mohd Isa, and Mohammad Indera bin Aziz. “Fingerprint Biometrics Authentication on Smart Card.” In: *2009 Second International Conference on Computer and Electrical Engineering* (2009), pp. 671–675. DOI: 10. 1109 /ICCEE. 2009.155.

[4] Ravi Shekhar Tiwari, Tapan Kumar Das, Durgashri G, and Arati Mohapatro. “A Smart Locking System Based on Multimodal Biometrics Authentication.” In: *IEEE 2024 5th International Conference on Circuits, Control, Communication and Computing (I4C)* (2024), pp. 571–576. URL: https://doi.org/10.1109/I4C62240.2024.10748442.

[5] C. O. Akanbi, I. K. Ogundoyin, J. O. Akintola, and K. Ameenah. “A Prototype Model of an IoT-Based Door System Using Double-Access Fingerprint Technique.” In: *Nigerian Journal of Technological Development* 17.2 (2020), pp. 142–149. URL: http://dx.doi.org/10.4314/njtd.v17i2.10.

[6] Arvind R. Ghosh, Meghna R. Raheja, and Rahul S. Kannoujiya. “IoT Based Anti-Theft Security System Using Biometric and Mail Notification.” In: *International Journal of Research Publication and Reviews* 5.5 (May 2024), pp. 11156–11162. URL: https://www.ijrpr.com/.

[7] A.Aditya Shankar, P.R.K.Sastry, A.L.Vishnu ram, A.Vamsidhar, International Journal of Engineering and Computer Science (IJECS) “Finger Print Based Door LockingSystem” vol.4, issue03, december2015 (Reference).

[8] Manish Aggarwal, Department of Electronics and Communication Engineering , Elins International Journal of Science Engineering and Management ”Secure Electronic Lock Based on Bluetooth Based OTP System”vol.2, Issue1, January 2017.

[9] R.Ramani, S.Valarmathy, Dr. N.SuthanthiraVanitha, S.Selvaraju,M.Thiruppathi, R.Thangam, “Vehicle Tracking & Locking System Basedon GSM & GPS”, I.J.Intelligent System and Applications, 2013,09,86-93.

[10] Anil K. Jain, Arun Ross and Salil Prabhakar. “An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics”, Vol. 14, January, 2004.