iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49673

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Multi-layer Anti-Theft System with an Intruder System

Rakshit Najbile[1], Twinkle Rawalani[2], Vedant Panda[3], Pratyush Mishra[4], Dr. Prasanna Deshpande[5]
[1, 2, 3, 4]*Student, (Electronics and Communication Department, Shri Ramdeobaba College of Engineering and Management, Nagpur)*
[5]*Assistant Professor, (Electronics and Communication Department, Shri Ramdeobaba College of Engineering and Management, Nagpur)*

Abstract: People are more concerned about the safety of their valuables like jewelry, money, important documents, etc. which is why safe deposit boxes are the safest place to keep them.
The advent of rapidly growing technologies enables users to operate high security systems with electronic identification options. In this work, a design of a multilayer security system is proposed. The safety concern parameters like user password, RF identification, and fingerprint recognition, use of one time password and a motion detection and alert system are in place. An email notification of the motion detection image near the safe may also be received by a user. Our system may be considered as a useful multi layered security anti-theft product.
Keywords: Multilayer, Fingerprint, OTP, Motion Detection, Alert System

I. INTRODUCTION

Digital revolution has significantly altered the life of mankind. Our lives are shaped and made easier by the constantly changing Landscape of modern technology and the innovation contained within it. Technology surely simplifies the details of our lives, it is equally crucial to uphold standards for safety and security.

The smart safe deposit boxes combine the best of both worlds' convenience and security, making them an interesting breakthrough for businesses, community centers, and multi-family housing situations in terms of convenience, security, safety, and effectiveness [1]. Smart lockers are becoming common all over the world [2].

The "modern and smart" security systems cost a fortune to set up, operate, and maintain due to the nature of software design, type of materials used, etc. However, they do cover other potential threats and function intelligently by incorporating other forms of alarms, particularly phone-based alarms for remote monitoring.

The evolution of safe deposit boxes starts with the invention of mechanical locks which are not highly secured due to forgery of keys. As technology improved, modern electronic locks emerged to prevent further unauthorized access and theft. One of the contemporary electronic locking systems that use a password as an authentication factor is the password-based locking system [2]. Next came the electronic lock system, which is an RFID-based system. The key components are RFID tags and readers, with the RFID value acting as an authentication factor [3].

Later, a cryptographic-based locking system was introduced that encrypted the original password to generate a new password. There are many other methods that work with the help of smart phones and networks, such as Wi-Fi , IOT and Near Field Communication (NFC) based lock systems [4].

Modern technology is now used to protect the locking system against OTPs. After that, further development of biometric locking systems such as face, fingerprint and voice has taken place [5]. Biometric systems have over time served as robust security mechanisms in various domains.

The earliest and most used biometric identification method is fingerprinting. Since over a century ago, law enforcement has used fingerprints to identify people. Personal authentication, such as gaining access to a computer, network, ATM, car, or home, is a much more widespread use of a fingerprint [6]. Electronic lock using fingerprint recognition system is a process of verifying the fingerprint image to open the electronic lock.

This project highlights the development of multiple layers of authentication where verification is completed by comparing the data of users by taking input from the user which will undergo the comparison process to compare with authorized data. Proposed system is implemented by utilizing two hardware which are authentication systems and an intruder System, where each hardware majorly contributes to make the system highly safe and secure.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

II. METHODOLOGY

The Multilayer security System is designed using Arduino Nano Controller, RFID module(RC522), LCD module, Fingerprint sensor (R307), 3x4 Matrix Keyboard, Ultrasonic Sensor (HC-SR04), GSM module (SIM800-WB64) and Servo motor as shown in Figure 1.

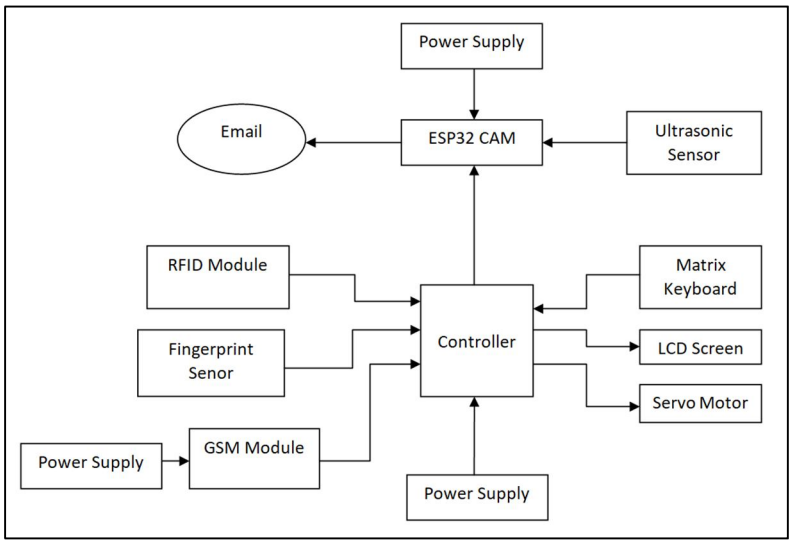


Figure 1: Multi Layer Anti theft system Block diagram

The Different stages which are used in the proposed device with respect to system flow as shown in Figure 2. As discussed system operation is achieved using two hardware which implementation has shown in Figure 3(a) and Figure 3(b):

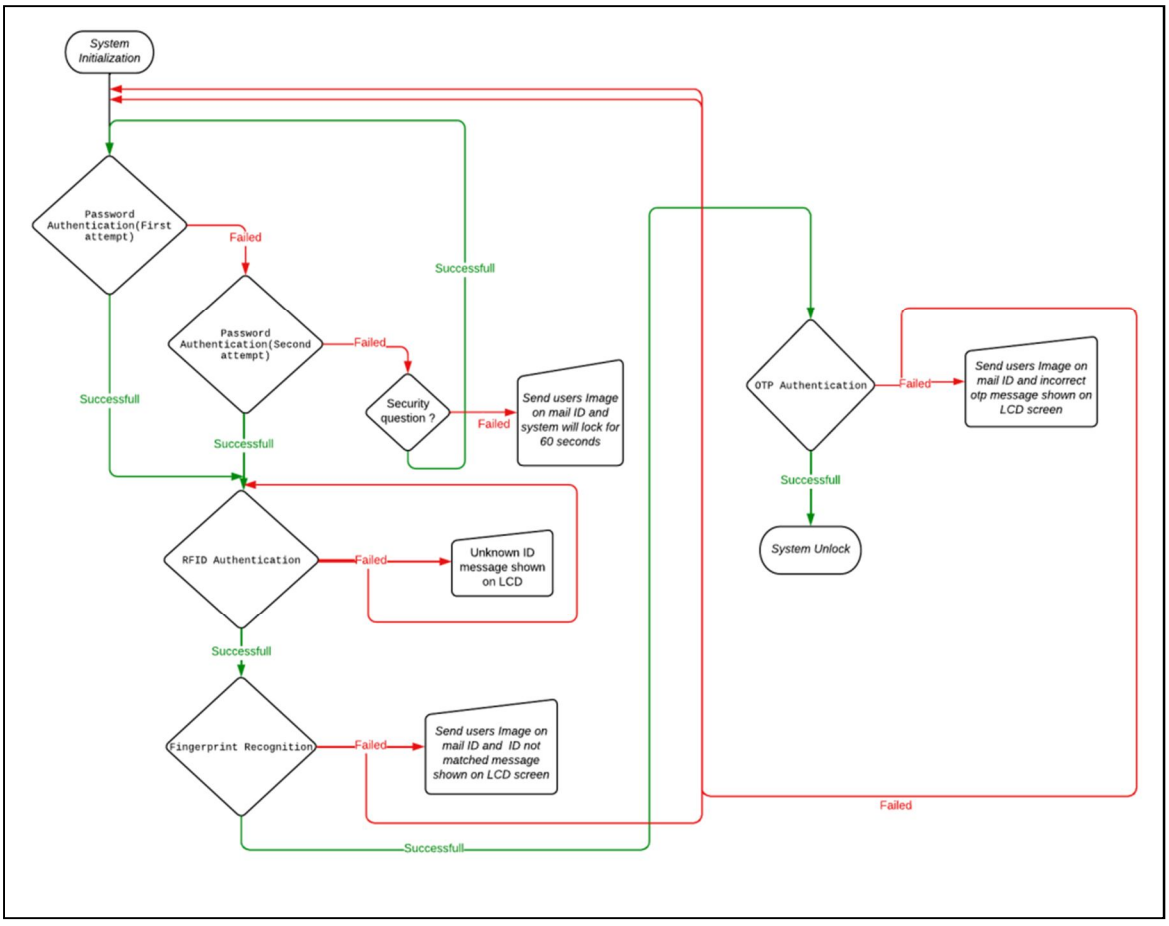


Figure 2: Multi Layer Anti theft system System flow

A. Authentication System

System authentication is distributed in different layers which are covered below:

1) *Layer 1:* For password enrollment user password is saved in code only which is dumped in Arduino nano. On powering the system it displays the Multilayer safe message on the LCD screen. Authentication begins by asking password to user, two attempts was given to the user if user enter the password in any of the given attempt correctly then second level of authentication begins and if failed in both attempts security question asked to the question if it is correct user gets another two attempt to enter the password and if it is wrong user image is captured and send on the mail id and system will locked for 60 sec, at this time all authentication layer is blocked.
2) *Layer 2:* For enrollment of the RFID card we upload the code. This code was available in Arduino IDE (after installing the RFID library). We approximate the RFID card to the reader until all the information is displayed on the serial monitor. After getting UID added this into the authentication code, for multiple users same procedure has done for enrolling RFID card. Secondary authentication begins with the RFID scanning. Radio waves are used by RFID to convey signals that turn on tags, which operate on the electromagnetic field principle. Once the card is valid at that point the system will inquire the user to proceed with the next step. RFID is communicating with Arduino Nano with SPI protocol for sending and receiving information.
3) *Layer 3:* For enrollment of the fingerprint we need to install the Adafruit Fingerprint Sensor Library then uploaded the enrollment code and open the serial monitor at a baud rate of 9600. We need to enter an ID for the fingerprint enrollment. For first fingerprint, we type 1 at the top left corner, and then, click the Send button. After that place a finger twice on the scanner for successfully saving into system. Similarly other fingerprint data is also enrolled. In this layer an optical fingerprint scanner scans the fingerprint of the user, every RFID is associated to one finger print after authentication the user can proceed to the OTP stage, if in case the fingerprint doesn't match with the associated RFID a Invalid user message will be shown on the LCD and an image of the same will be captured by the ESP32 CAM and will be send to the designated email for activity recording as shown in Figure 4. The operation of the fingerprint sensor is based on the total inner reflection (TIR) concept. For the TIR to occur, light from a source must be allowed to penetrate through one face of the prism at a specific location. To deliver digital images, the scanner uses a microchip (CMOS picture sensor). This fingerprint scanner includes two forms: one is unique fingerprint enrollment, and another one is fingerprint matching. Initially the fingerprint enrollment is done and all the fingerprints are stored in the form of source copy. For this R307 scanner, each module should recognize the address. When this module communicates with the system, each information source is exchanged within the information package frame containing the address thing. The scanner reacts as if it were that information package whose value matches the address value of the scanner.
4) *Layer 4:* In this layer OTP will be generated and is sent to the registered mobile number, where the GSM module is used to send SMS. For assigning the mobile number of each user for OTP authentication we are overwriting a variable which is created to store the mobile number of a user, so as soon as any user scan the RFID we get UID of user so we are overwriting the variable with the mobile number of the user based on the ID fetched from the RFID and it pass to the designated function which does further operation. The Arduino will communicate with the GSM module by using AT commands and sends MESSAGE to the associate mobile number. AT+CMGS is used to send SMS message. If an OTP doesn't match, the system automatically sends an Image of the activity to the designated email immediately using ESP32CAM as shown in Figure 4. After checking the correct OTP system will show unlock indication on the LCD screen and rotate the servo motor by 90 degree.

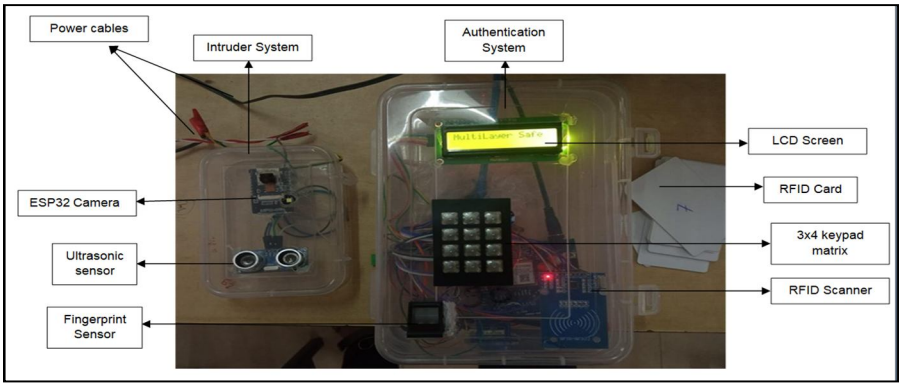


Figure 3 (a): Implemented system front side

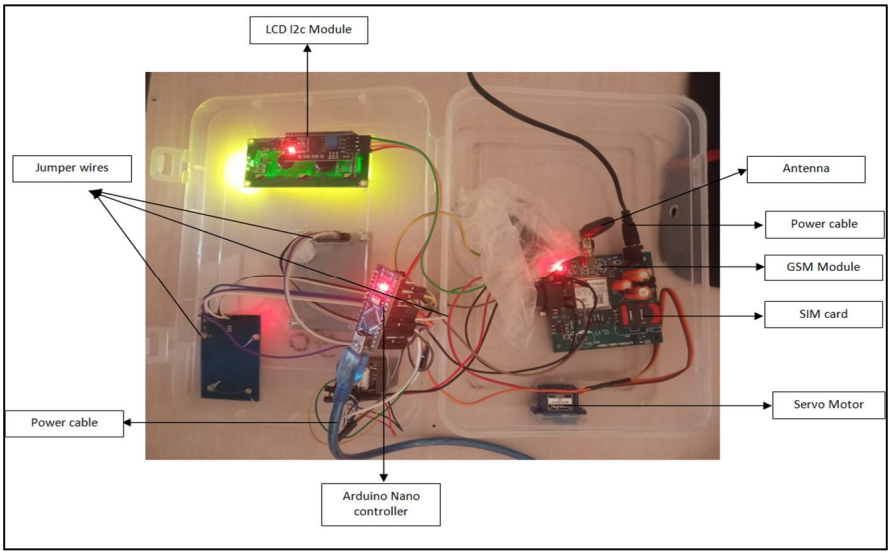


Figure 3 (b): Implemented system backend

B. Intruder System

The system uses an ESP32-CAM camera module and an ultrasonic sensor for movement detection. The ESP32-CAM is a low-cost microcontroller that integrates Wi-Fi and Bluetooth connectivity, and has an onboard camera module that can capture images. As this system initializes it starts to detect for any Motion nearer the safe deposit system, it would be detected by using the ultrasonic sensor. In this system the threshold value has been set up to 50 cm and thus it continuously monitors the surroundings up to the safe deposit system. If some Motion is found nearer the safe deposit box and on incorrect password attempts the system will send an image to the designated email immediately shown in Figure 4.This allows the system owner to be alerted in real-time of any unauthorized access attempts and take appropriate action. The ESP32 MailClient library is used to send emails with the ESP32-CAM, which must be connected to the internet. With the help of this library, the ESP32 CAM can send and receive emails over SMTP, with or without attachments. For this project, sending an email with an attachment requires the use of SMTP. SMTP implies Simple Mail Transfer Protocol and it is an internet standard for e-mail transmission.

III. RESULTS AND CONCLUSION

The multi-layered anti-theft system was successfully implemented and tested in various scenarios to evaluate its performance. The following section provides a detailed analysis of the results and a discussion of the findings.

Password-based authentication remains one of the most commonly used security measures for digital systems and applications due to its simplicity and familiarity among users. We found that user education and awareness about password security best practices played a significant role in the effectiveness of password-based systems. Users who were educated about the importance of using unique and complex passwords and avoiding password reuse were more likely to choose strong passwords and maintain good password hygiene. In our study, we found that security questions were most effective when they were paired with a strong password policy that encouraged users to choose complex and unique passwords. This helped reduce the risk of brute-force attacks and guessing of security question answers, password authentication layer interface has shown in figure 4.

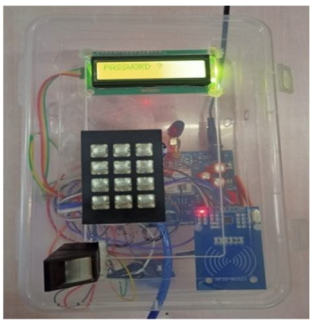


Figure 4: Password Authentication interface

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

The performance of the RC522 RFID module-based authentication layer was effective in identifying and authenticating tags. The system was able to read tags accurately at distances of up to 10 cm, and the orientation of the tags did not significantly affect the performance of the system. The system has been tested against multiple RFID cards which gives significant performance, RFID Authentication layer interface has shown in figure 5.

Figure 5: RFID Authentication

The results of the study showed that the R307 fingerprint sensor-based authentication layer was effective in identifying and authenticating fingerprints. The system was able to enroll and recognize fingerprints accurately, with an average recognition time of less than 5-10 second; the fingerprint-based authentication component was tested by capturing and verifying a large number of fingerprints. The system achieved an good accuracy, which demonstrates its ability to accurately and reliably verify user identities using fingerprints. Fingerprint based authentication provides great stability and it is difficult to create fake identity based on biometric image which provides robustness to the system, Fingerprint Authentication layer interface has shown in figure 6.

Figure 6: Fingerprint Authentication

The OTP-based security system using the SIM800-WB64 GSM module was effective in providing additional security. The system was able to generate and send OTPs accurately and quickly and send them to the user device via SMS. The user device was able to enter the OTP and send it back to the microcontroller for authentication, with an average authentication time of less than 5 seconds. The system was also able to detect and prevent phishing attacks, and replay attacks were ineffective due to the OTP's one-time use. The system was also able to operate reliably in different network environments, including areas with low signal strength. This Layer was tested by generating and verifying a large number of one-time passwords. The system achieved an good success rate, which indicates its ability to securely and efficiently verify user identities using OTPs, OTP Authentication layer interface has shown in figure 7(a) and figure 7(b).

Figure 7(a) : OTP Authentication (SMS sent interface)

Figure 7(b) : OTP Authentication (Enter OTP interface)

The Intruder System which was effective in detecting intruders and sending alerts via email using ESP32 CAM and Ultrasonic sensor HC-SR04. The system was able to accurately detect unauthorized access by monitoring motion near the safe deposit boxes within the range of 50 cm and also detect incorrect password attempts which indication is sent by the controller to the ESP32 CAM . The system was able to send email alerts to the designated email address via an SMTP server, indicating the image of the user who is currently trying to access the system and it has been found that the system takes an average time of 5-10 sec to send the image.
Below table 1 we have tried to explain how effective our proposed solution is over existing solutions by comparing some parameters such as hardware Cost efficiency and Security layers.

Table 1. Comparative analysis:

Approach	Cost efficiency	Security Layers
Our Approach	1. Based upon the components used in this project cost is around 4000 rs. 2. Per layer cost is 650 rs.	Authentication system layers: 1. Password authentication 2. RFID authentication 3. Fingerprint recognition 4. OTP authentication Intruder system layers: 1. Alert notification (sending image of user to authorized person email id on incorrect attempts) 2. Movement Detection
"Bank Locker System" Internet of Things (IoT) [7]	1. Based upon the market survey the added estimated cost of this project is around 3300 rs. 2. Per layer cost is 1650 rs	Authentication system layers: 1. Password Authentication 2. Face recognition Intruder system layers: 1. Alert notification (Sending message on authorized person mobile number) 2. Movement detection

Six Tier Multipurpose Security Locker System Based on Arduino [8]	1. Based upon the market survey the added estimated cost of this project is around 7230 rs. 2. Per layer cost is 1250 rs.	Authentication system layers: 1. Password authentication 2. Fingerprint recognition Intruder system layers: 1. Alert notification (Sending user location and time to authorized person.) 2. Movement detection
Bank Locker Security with Fingerprint and Image Capture[9]	1. Based upon the market survey the added estimated cost of this project is around 5050 rs. 2. Per layer cost is 1680 rs.	Authentication system layers: 1. Fingerprint recognition 2. Face recognition Intruder system layers: 1. Alert notification (Sending message to the authorized person.) 2. Movement detection

The per hour power consumption of the whole system has been shown in the table 2. We have calculated the power consumption with the assumption of system is used 5 times in an hour.

Table 2. Installed modules power consumption:

Components	Power consumption in A/h
Arduino Nano	25.5mA/s *60 sec*60min =91.8 A/h
GSM module	1mA/s *60 sec*60min =3.6 A/h
RFID module	20mA/s *60 sec*60min =72 A/h
Fingerprint Sensor	75mA/s *10 sec*5 times =3.75 A/h
ESP32 camera	20mA/s *60 sec*59 min +310mA*9 sec (Let's assume image capture for 2 times which takes approximately 9 Sec) =73.59 A/h
LCD screen	20mA/s *60 sec 60 min =72 A/h
Keypad	30 mA/s *60 sec*2 min =3.6 A/h
Ultrasonic sensor	15 mA/s *60 sec*60 min =54 A/h
Servo motor	2 A/s *5 Sec(5 sec on)*5 times = 50 A/h
Total	= 424A/h

It is worth noting that the proposed system collectively provides more robustness in terms of security provided by the existing system by combining multiple layer Authentication System and Intruder System as well as the time consumption by the each layer to process is very less and the system accuracy which we get because of the dedicated module is really a great.

REFERENCES

[1] Crystalynne D. Cortez, Jaswinder S. Badwal, Jocelyn R. Hipolito, Ditche Jane C. Astillero, Melvie S. Dela Cruz, and Jaira C. Inalao, "Development of Microcontroller-Based Biometric Locker System with Short Message Service", Lecture Notes on Software Engineering, Vol. 4, No. 2, May 2016.

[2] Rahman, Md M. and Ali, Mohammed S. and Akther, M. Shoaib, "Password protected electronic lock system for smart home security", International Journal of Engineering Research and Technology,Vol 7,No. 4, pp. 541-544,2018.

[3] R.Ramani, S. Selvaraju, S.Valarmathy, P.Niranjan, "Bank Locker Security System based on RFID and GSM Technology", International Journal of Computer Applications, November 2012.

[4] Vinay N. S. , Pruthviraj A. S., Karan S. S., Manu N. R., S. R. T., "Smart Locking and Unlocking System for ATM Trunk." , International Journal of Research in Engineering, Science and Management Volume-1, Issue-12, December-2018.

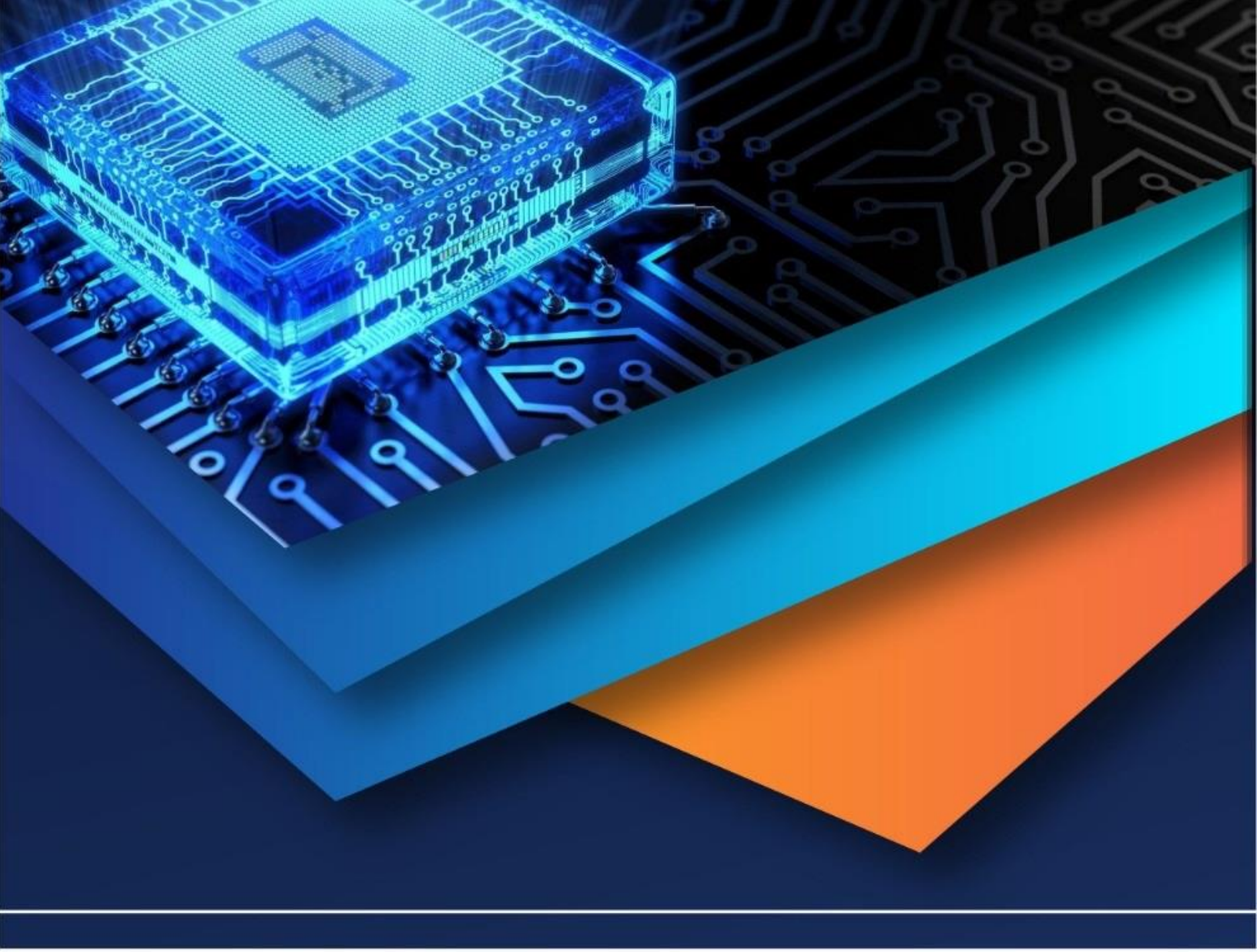
[5] S. Asha , C. Chellappan , "Biometrics: An Overview of the Technology, Issues and Applications", International Journal of Computer Applications Volume 39–No.10, February 2012.

[6] Aditya Sanskar, P.K.R Sastry, A.L Vishnu Ram, A.Vamsidhar , "Fingerprint Based Door Locking System",International Journal Of Engineering And Computer Science, March 2015.

[7] Prof Garande, Prachi Bharne, Mansi Shah, Tejal Joshi, and Siddhant Chaudhary, "Bank Locker System" Internet of Things (IoT)," International Journal of Advanced Research in Science, Communication and Technology, vol. 2, no. 4, pp. 513-515, Apr. 2022.

[8] A. Z. M. Tahmidul Kabir, Nirmol Deb Nath, Utshaw Rafin Akther, Fukrul Hasan, and Tawsif Ibne Alam, "Six Tier Multipurpose Security Locker System Based on Arduino," 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT),pp. 1-5, 2019.

[9] V. Hindumathi, M. Sushmitha, M.Yoshitha, R. Venkata Harika, A. Sri Vaishnavi, "Bank Locker Security with Fingerprint and Image Capture", Journal of Electronic Design Engineering Volume 5 Issue 2,pp. 19-24, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY