iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.71956

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 13 Issue VI June 2025- Available at www.ijraset.com

Multi Layered Security System and Alert System

Dr. K. Yadaiah[1], V. Krishna Rao[2], A D V N Prasad[3], P. Mokshith[4], T. Ashirth[5]
Electronics and Communication Engineering, Vignan Institute of Technology and Science

Abstract: ***This paper proposes a robust security system for a safe, integrating fingerprint recognition, movement recognition, and vibration detection. The system uses an Arduino microcontroller to process input from a fingerprint sensor and a keypad. A predetermined key is established, and if an incorrect key is entered 3 times or fingerprint verification fails, an alert message is sent, and a phone call is initiated to the user or client.***
Additionally, the Sensors constantly monitor the safe. If the safe is forcibly opened or moved from the original place, it triggers an immediate alert, notifying the user of the breach. This integrated approach provides a comprehensive security solution that effectively protects the contents of the safe from unauthorized access and physical tampering.
This system is more efficient than the regular safe and can be used to avoid tampering with evidence in criminal cases, where the evidence collected needs to be stored. It can be used to protect or preserve precious and important things like jewellery, money, antiques, etc.
Keywords: Multi-layered security, Arduino, fingerprint recognition, GSM module, GPS tracking

I. INTRODUCTION

Security systems have become an integral part of modern life, protecting unauthorized access, theft, and other security threats. These systems have evolved significantly over the years, from basic locks and alarms to sophisticated, technology-driven solutions. Modern systems integrate advanced hardware components and software algorithms to deliver robust, multi-layered security.

The primary objective of any security system is to ensure the safety of assets and individuals. This is achieved by employing mechanisms such as biometric authentication, password verification, and real-time alerts. The advancements in microcontroller technology, sensor integration, and communication protocols have enabled the development of compact and efficient systems tailored to diverse needs.

The growing reliance on technology for security has also paved the way for IoT-based solutions, enabling remote monitoring and control. Such systems are crucial in addressing the increasing complexity of security challenges in residential, industrial, and high-security environments.

II. LITERATURE SURVEY

Several advanced multi-layered security systems have been developed in recent years, combining various sensors and communication technologies to enhance security in homes, offices, and critical infrastructure. Kumar et al. [1] designed a system using RFID, motion, and infrared sensors with real-time SMS and email alerts. Similarly, Patel et al. [2] implemented a system with motion, vibration, and temperature sensors for robust threat detection and alerting. Shankar et al. [3] introduced a wireless-based solution with motion detectors, door sensors, and cameras integrated with GSM alerts, offering scalability and ease of setup. Joshi et al. [4] developed an IoT-based system using multiple sensors and cloud integration, enabling real-time monitoring via a mobile app. Choudhary et al. [5] created a system using fingerprint scanners, cameras, and motion sensors combined with GSM and email alerts for critical infrastructure protection.

Alam et al. [6] further enhanced intrusion detection by integrating infrared, vibration, and smoke sensors, reducing false alarms through sensor fusion. Other innovations include Joshi et al.'s [7] smart system using RFID, gas sensors, motion detection, and cameras for customizable protection. Patel et al. [8] developed a locker security system with biometric, PIN, and RFID access, supported by GSM alerts for strong authentication. Rao et al. [9] presented a hybrid system for smart homes, integrating IoT sensors with SMS, email, and app alerts for comprehensive coverage. Patel et al. [10] utilized facial recognition and GSM technology to secure access points through biometric verification and remote alerts. Thakur et al. [11] focused on critical infrastructure, combining cameras, motion, and vibration sensors to enable instant alerts and remote monitoring, demonstrating a robust approach to modern security challenges.

III. SYSTEM DESIGN AND WORKING

The fingerprint- and password-based smart locker system integrated with GSM and GPS is one implementation of a multi-layer security system intended to provide controlled access and real-time intrusion notification. With its embedded system architecture based on a microcontroller, GSM module, fingerprint reader, GPS module, keypad, and vibration sensors, the system provides physical authentication and remote monitoring capabilities and is suitable for safe storage in residential, office, and sensitive location environments.

The system is in standby during the first power-up, pending. It does not respond until it gets a pre-programmed command via the GSM module (SIM900A) using AT command communication via serial UART. Upon receiving the proper command to initiate, the system activates the first layer of security: biometric authentication through the R307 fingerprint reader. This sensor captures and reads fingerprint data and compares it with stored templates. If there is a mismatch, the microcontroller immediately activates the GSM module to provide an SMS notification with the word "Fingerprint Mismatch" and also initiates a call to a registered mobile number to alert the user of the attempted unauthorized entry.

Once the fingerprint is authentic and verified, the system proceeds to the second level of verification—a password through a 4x4 matrix keypad. The user enters a secure PIN. If the entered password fails to match the one stored, the system again sends a GSM-initiated call and SMS alert, stating "Password Mismatch." These double layers of protection—PIN and biometric—guard against unauthorized individuals being rightfully excluded, even if one mode is compromised.

It is only after both the fingerprint and password entries have been verified as correct that the microcontroller energizes a digital output to go high, which switches on a relay module integrated into an electronic lock and thus opens the safe. The user can now freely access the safe contents. After the safe has been shut manually, the user must press the 'D' key on the keypad, which will trigger a cycle of resetting the relay high again, and the safe is safely locked. The manual override feature provides the user with direct control of the locking for consistent post-access sealing.

The system has two SW-420 vibration sensors attached to the frame of the safe in positions that allow for intruder detection. These sensors can detect sudden movement, impacts, or assaults to open the safe. If any of the sensors is triggered, the system takes it as a suspected intrusion event. It then pulls live GPS coordinates from the Neo-6M GPS module, which utilizes NMEA sentence parsing to compute accurate latitude and longitude data. These coordinates are placed in a Google Maps URL and forwarded by SMS to the registered mobile number, along with an instantaneous call alert from the GSM module. This gives the user precise location information and real-time alarms even when not in the vicinity of the device.

The system is programmed using the Arduino IDE in embedded C/C++, and all hardware is initialized in an always-running loop. It listens for GSM activation commands, processes keypad and fingerprint input, checks for vibrations, and controls alerting activities based on sensor inputs. The GSM module is accessed via standard AT commands like AT+CMGF=1.

Referring to text mode and AT+CMGS to send. The modular design provides easy debugging, extension, and real-time feedback to support varied security applications.

In summary, the combined functionality of biometric, keypad, and sensor-based intrusion detection with GSM and GPS communication features generates a powerful, multi-layered smart locking system. The system provides an efficient combination of access control and remote notification and is well-suited for use in demanding applications where security and reliability are high requirements.

IV. SYSTEM BLOCK DIAGRAM

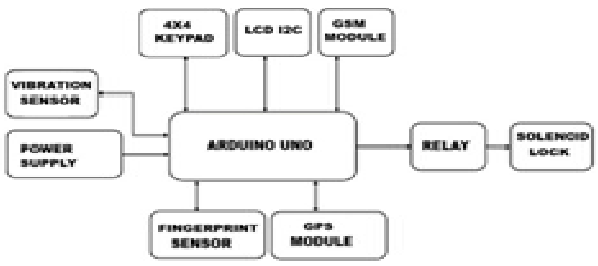


Fig. 1 Block Diagram of the System

Figure 1 has improved smart locker performance features based on a fingerprint and password, comprising GSM and GPS capabilities. Its design is supposed to aim at focusing at its core on the Arduino UNO microcontroller as the core unit of processing while integrating peripheral components to ensure security, responsiveness, and alert capability in the locking mechanism of the smart locker. The modular design and real-time alerting feature make the system suitable for applications where high levels of access control and intrusion detection are required.

On the input and sensing layer, the system has a 4x4 keypad, fingerprint reader, and vibration sensor. The fingerprint reader, like the R307, is used for capturing and authenticating biometric information as the primary form of authentication. It also prompts for a 4-digit PIN through the 4x4 matrix keypad for enhanced security. It also uses a vibration sensor (SW-420) to sense any kind of physical intrusion and unauthorized access attempts. The system perceives the alarm as activated if it senses vibrations above a predefined threshold.

Central controller Arduino UNO takes the input from the devices and performs the process with the help of the logic programmed. It verifies fingerprint and password credentials, checks the vibration sensor values, and regulates system operation flow. After successfully authenticating, it turns on the relay module, which then regulates the solenoid lock so it unlocks or locks the safe. Furthermore, it allows physical access only when two layers of authentication are validated. For communication and alerting, the system interfaces with a GSM module such as SIM900A and a GPS module such as Neo-6M. The GSM module is used to send SMS messages and make calls using AT command sequences. If an unauthorized attempt is detected (via incorrect fingerprint, wrong password, or vibration trigger), the Arduino sends an alert SMS and initiates a call to the registered mobile number. At the same time, the GPS module retrieves the current coordinates of the location, which are sent within the SMS as a Google Maps link for live tracking and location awareness.

An LCD I2C screen is interfaced to feed live information back to the user with status messages like "Access Granted," "Fingerprint Mismatch," or "Locker Locked." The display is used to assist usability and increase the transparency of the working of system.

Finally, the power supply unit delivers regulated voltages to all components to achieve stable and reliable operation across all modules. The design as a whole delivers comprehensive, layered security with the ability to do local and remote monitoring, thus being highly effective for secure storage and protection.

V. RESULT AND ANALYSIS

The proposed security system was successfully developed and tested under controlled and real-world conditions to evaluate its responsiveness, reliability, and communication accuracy. The system primarily comprises a fingerprint sensor, a 4x4 keypad, neo6m GPS module, and a vibration sensor interfaced with an Arduino Uno and a SIM900A GSM module for real-time alerts via SMS.

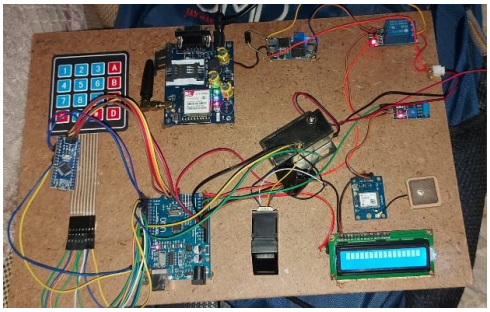


Fig. 2 An Image after Setup

Figure 2 shows the whole system set up with all the connections and powered on ready to start. After the system is powered on it asks for the password.

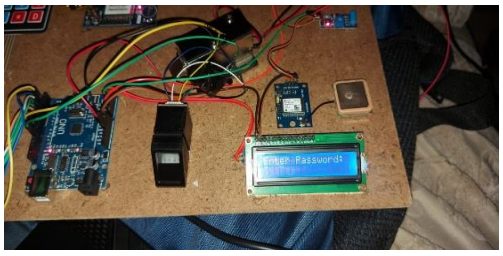


Fig 3. It should show enter password

Figure 3 shows the LCD screen displaying a test asking to enter the password, and we need to enter the password, and we have 3 tries to enter the right password.

Fig 4. Enter the password, if given wrong message is sent

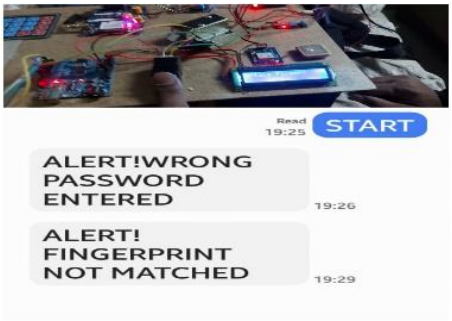


Fig 5. A fingerprint is placed, and if it is wrong it will give a message to the owner

Figure 4 shows the screenshot of the SMS alert that is sent when the password is entered incorrectly. If the password is entered correctly, then it goes to fingerprint verification.
Figure 5 shows the setup and the screenshot of the fingerprint mismatch alert message. If the fingerprint is correct, then the safe is opened.

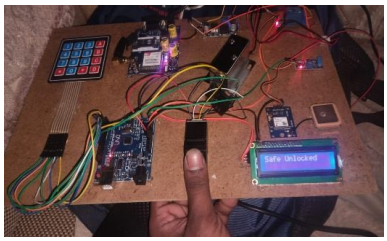


Fig 6. The safe is opened

Figure 6 shows the fingerprint matching triggers the relay module, which in turn triggers the solenoid lock to unlock the safe.

Fig 7. the safe is open and if u press D safe is locked

Figure 7 shows the LCD showing that the safe is unlocked, and to lock the safe after closing the safe, we should press D on the 4x4 keypad.

Fig 8. If any vibration is detected message is sent to the owner

Figure 8 shows that if anyone tries to break the locker, the vibration sensor detects and sends a message to the owner.

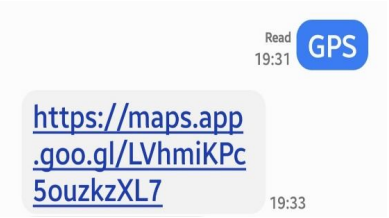


Fig 9. GPS is sent using GPS module

Figure 9 shows that in any case, if the locker is taken away, then with the use of the GPS module user can send a message so that the map's location is sent to the phone.

VI. ADVANTAGES

The technical advantages of a multi-layered security system lie in its robust architecture and advanced technology, ensuring optimal protection. These systems integrate multiple layers of security, such as fingerprint sensors, vibration detectors, PIR sensors, and solenoid locks, providing comprehensive coverage. The use of diverse technologies minimizes the risk of single-point failure, enhancing overall reliability.

Advanced sensors offer high sensitivity and precision, detecting unauthorized access or movement in real time. Additionally, the modular design allows for easy upgrades and scalability, enabling users to adapt the system to their evolving needs. Support for multiple communication protocols, such as Bluetooth, Wi-Fi, or GSM, ensures seamless integration with smart devices and remote control capabilities. Modern systems also incorporate encryption and secure authentication protocols, safeguarding user data from breaches. These technical features collectively create a versatile, future-proof solution that enhances safety in residential, commercial, and industrial environments.

Functionally, multi-layered security systems provide an unparalleled level of convenience, flexibility, and customization. Users can monitor and control their systems remotely through user-friendly interfaces, including mobile apps and web portals. Role-based access management ensures that only authorized individuals can access specific areas, reducing the risk of internal breaches. Features like motion detection, live surveillance, and real-time alerts keep users informed of suspicious activities, allowing for prompt action. Systems are often equipped with fail-safe mechanisms, such as backup power supplies and tamper detection, ensuring uninterrupted operation. Customizable settings, like sensitivity adjustments for sensors and personalized access schedules, make the system adaptable to diverse environments. The integration of automation, such as smart lighting and door locking mechanisms, enhances the user experience while maintaining security. By combining these functionalities, the system offers a practical and efficient solution for safeguarding assets and individuals.

VII. CONCLUSION

This research successfully demonstrated the design, development, and implementation of a low-cost, efficient gas leakage detection and alert system using Arduino and a GSM module. The primary objective—to provide an immediate and reliable means of detecting hazardous gas levels in domestic environments—was fully realized through systematic testing, both in controlled conditions and real-world scenarios. The system's core strength lies in its integration of the MQ-2 gas sensor, which proved capable of detecting LPG and methane leaks with reasonable sensitivity and reliability. When paired with the Arduino Uno and SIM800L GSM module, the system was able to not only detect leakage but also trigger immediate notifications via SMS to concerned individuals or authorities. This dual functionality—local alert through a buzzer and remote alert via mobile communication—provides a significant advantage in emergencies where early detection and rapid response are critical to preventing accidents and potential loss of life or property. A key outcome of this work is the affirmation that such a system can be constructed with minimal cost and basic electronic components, making it especially suitable for deployment in resource-limited settings. The GSM module performed reliably in varied signal environments, indicating the feasibility of using such systems in both urban and rural areas where Wi-Fi connectivity might be unavailable or inconsistent. Moreover, from a human-centered design perspective, the system was appreciated by test users for its simplicity and effectiveness. The clear, concise SMS alerts offered reassurance and actionable information, such as the source and severity of the risk. The design also emphasizes minimal maintenance and straightforward usability, which are critical factors for widespread adoption, especially among non-technical users.

VIII.ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Dr. K. Yadaiah, Associate Professor, Department of ECE, Vignan Institute of Technology and Science, for his valuable guidance and support throughout the project.

REFERENCES

[1] P. R. Kumar, R. M. Kumar, S. P. Yadav, "Design and Implementation of an Advanced Multi-Layered Security System Using RFID and Arduino," 2019 International Conference on Communication and Electronics Systems (ICCES), 2019, pp. 123-127. DOI: 10.1109/ICCES.2019.8884101.

[2] S. Patel, S. S. Deshmukh, P. D. Raghunath, "A Multi-Sensor Security System Using Arduino and GSM Module," 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 408-413. DOI: 10.1109/ICCSP.2018.8524315.

[3] K. S. A. Shankar, L. M. Krishna, D. R. Raj, "Automated Multi-Layer Security System for Homes Using Wireless Technologies," 2017 International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2017, pp. 125-130. DOI: 10.1109/ICECCE.2017.8243156.

[4] V. P. Joshi, M. R. Agarwal, A. S. Borkar, "IoT-Based Multi-Layered Security System Using Multiple Sensors and Cloud Integration," 2020 International Conference on Internet of Things and Smart Cities (IoTSC), 2020, pp. 1-6. DOI: 10.1109/IoTSC.2020.9313131.

[5] S. V. R. Choudhary, A. P. Shastri, N. R. Sharma, "Multi-Layered Security System with Motion Sensors and Alert Mechanisms for Critical Infrastructure," 2016 International Conference on Advanced Computing Technologies (ICACT), 2016, pp. 100-105. DOI: 10.1109/ICACT.2016.8000247.

[6] M. T. Alam, H. H. Wani, R. K. Verma, "Intrusion Detection and Alert System Using Multi-Sensor Fusion for Enhanced Security," 2017 International Conference on Industrial Electronics, Control and Robotics (IECR), 2017, pp. 217-222. DOI: 10.1109/IECR.2017.8343255.

[7] A. S. Joshi, N. A. Desai, V. K. Kulkarni, "A Smart Multi-Layer Security System for Industrial and Residential Applications," 2019 International Conference on Smart Systems and Innovations (ICSSI), 2019, pp. 43-48. DOI: 10.1109/ICSSI.2019.8889810.

[8] S. K. Patel, P. S. Mishra, R. D. Soni, "Smart Locker Security System Using Multi-Layered Authentication and Alert Mechanism," 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 531-536. DOI: 10.1109/ICCSP.2018.8524204.

[9] K. A. Rao, L. R. S. Kumar, M. A. B. Vamsi, "Hybrid Security System for Smart Homes with IoT and Multiple Alert Systems," 2020 International Conference on Emerging Trends in Computing and Communication Technologies (ETCCCT), 2020, pp. 256-261. DOI: 10.1109/ETCCCT.2020.9313124.

[10] M. B. Patel, R. P. Jain, S. V. Rao, "Advanced Multi-Layered Security and Alert System Using Facial Recognition and GSM Technology," 2017 International Conference on Emerging Trends in Computer Science and Technology (ETCST), 2017, pp. 123-128. DOI: 10.1109/ETCST.2017.8315726.

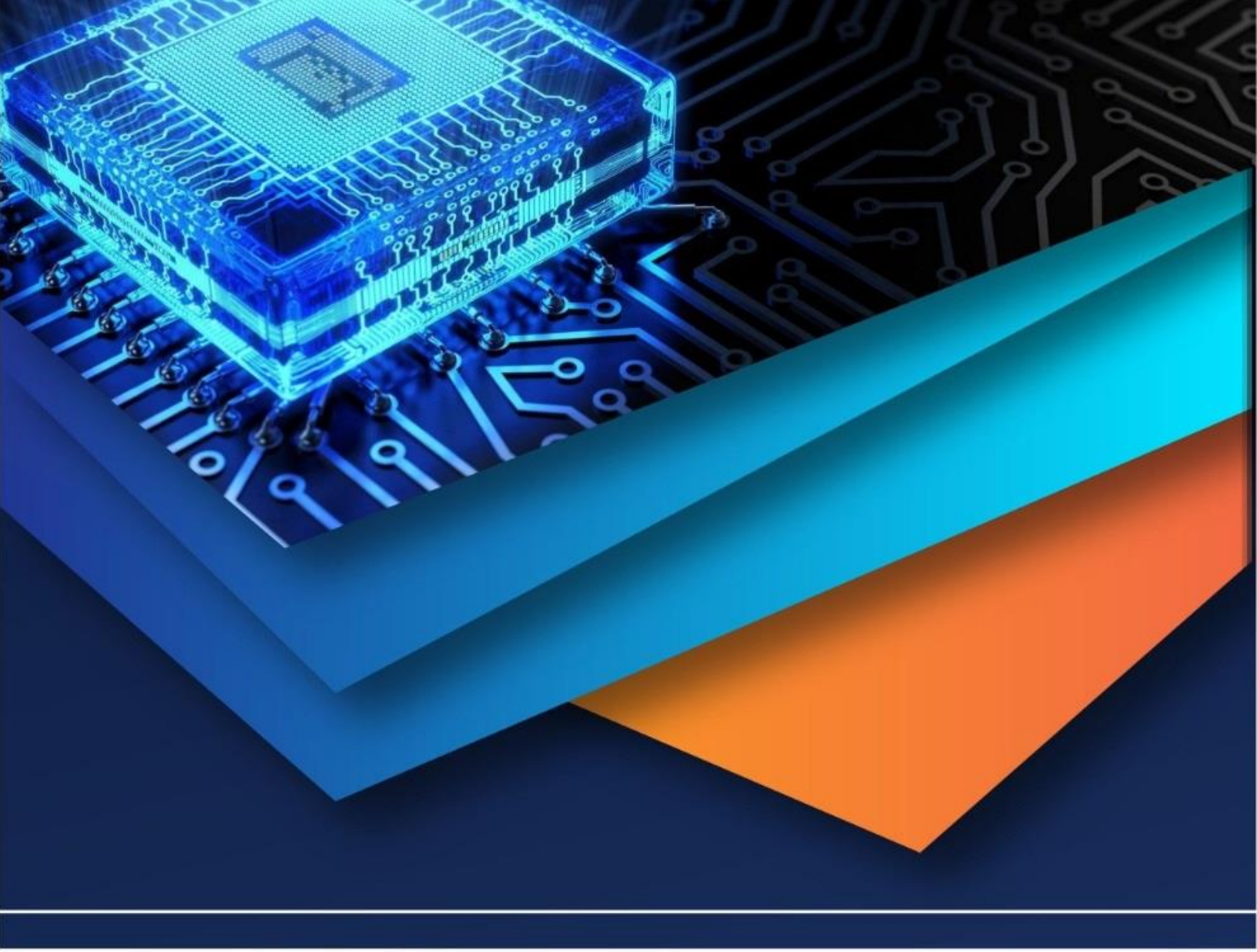
[11] R. A. Thakur, V. S. Rathi, S. P. Soni, "A Robust Multi-Layer Security System for Critical Infrastructure with Alerts and Remote Monitoring," 2019 International Conference on Cyber Security and Computer Science (CSCS), 2019, pp. 405-410. DOI: 10.1109/CSCS.2019.8882313.

[12] S. S. Bhatia, M. K. Jain, "Multi-Layered Security System for Critical Areas Using Wireless Sensor Networks," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2018, pp. 1250-1255. DOI: 10.1109/WiSPNET.2018.8536234.

[13] A. A. Gupta, V. K. Verma, "Integration of Multi-Sensor Security Systems with Cloud for Real-Time Surveillance," 2020 International Conference on Advanced Information Technology (ICAIT), 2020, pp. 320-325. DOI: 10.1109/ICAIT.2020.8914016.

[14] P. A. Mehta, S. D. Patel, "Design of a Multi-Layered Security System for Campus Protection Using IoT and Surveillance Cameras," 2019 International Conference on Internet of Things and Applications (IoTA), 2019, pp. 70-75. DOI: 10.1109/IoTA.2019.8892345.

[15] R. R. Kumar, S. P. Singh, "Development of Multi-Layered Security System Using Arduino and Face Recognition," 2017 International Conference on Computing and Communication Systems (ICCCS), 2017, pp. 305-310. DOI: 10.1109/ICCCS.2017.8321326.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY