International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Three Layer Advanced ATM Security

[1] P. Siva Kalyani,[2] Guvva Pravalika,[3] Shivaram Kathyayani,[4] Vasamsetty Karun Kumar,[5] Maddi Srinath Goud,

[1]Assistant Professor, Department of ECE, Narsimha Reddy Engineering Collage, Maisammaguda(V), Kompally, Telangana.

[2,3,4,5] Student, Department of ECE, Narsimha Reddy Engineering Collage, Maisammaguda(V), Kompally, Telangana.

Abstract—

Banks and other financial organizations are always looking for new ways to keep customers' money and valuables safe in their vaults, since security risks are always changing. This study investigates a thorough method for strengthening the security of bank lockers via the use of the Internet of Things (IoT) and several levels of authentication. Features like as real-time picture capture of illegal access attempts, fingerprint recognition, keypad password input, and one-time password (OTP) verification are all part of the suggested system. An easy and safe way to enter lockers is using fingerprint recognition, which guarantees biometric uniqueness. Having a keypad to enter a customized code is an extra security measure that gives peace of mind. One-time password (OTP) verification further fortifies authentication by reducing the likelihood of illegal access via the dynamic generation of time-sensitive codes. Enhancing security measures is greatly facilitated by integrating the IoT. The technology takes a picture of the invader and sends it to a manager's bot whenever someone tries to get in without permission. esponding and intervening promptly is made possible by this proactive alarm system. To further aid security managers in tracking and analyzing locker use trends, the system keeps an access history record. Bank locker security is enhanced and new threats are effectively countered by the suggested multi-layered authentication system that incorporates the internet of things. Customers will have more faith in banks as a result of this study's contribution to the continuing efforts to build enhanced security frameworks for protecting financial assets.

Security system for bank lockers; multi-layered authentication; one-time password verification; internet of things; proactive alarm system.

I. INTRODUCTION

The safest place to store valuables is in a bank locker. The increase in threats against banks is worrisome, however, since institutions are often the targets of illicit activities. Our banks' current procedures aren't particularly reliable, and anybody with a little ingenuity and evil in them could easily make them work. A customer can't open their bank locker without both of their keys, according to the present system. The first customer to unlock the bank's locker will get one key, while the bank itself will retain the other. The most significant drawback is that the person will be fined and paid for a new key if they happen to lose it. Various keyless strategies are presented in the articles to tackle these issues. An innovative system for bank lockers has been designed that requires a password to open the door. This system can simultaneously activate, authenticate, and verify the user, ensuring safe admission to the bank locker. The most fundamental benefit of using passwords is that they are more secure than other solutions [1]. A keypad is used to input the password for this system. If the user enters the wrong password, the intruder alarm will alert the wrong person [2]. A dynamic one-time password (OTP) is generated and only valid for a single login attempt. Using an OTP enhances the security of static password-based authentication methods [3]. However, there will be a new conversation about RFID cards in the event that the password is sometimes lost. A digital security

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

system may activate, authenticate individuals in real-time, and unlock doors for safe access by using a passive kind of RFID [4]. A GSM-enabled SMS is delivered to a legitimate individual whose ID number is read accurately by the RFID reader tag. The lock unlocks [5-6] if the password is correct. We run the danger of losing track of the RFID tag and no one can afford to use it. New biometric methods are being used in security system development. Biometrics are a collection of characteristics that are unique to each person and may be used to verify their identification. When it comes to common issues, the fingerprint-based lock is an excellent answer. The ability to access a system via the use of pre-stored fingerprints in memory is known as fingerprint recognition technology [7]. An alarm message is sent to the authorized person and the buzzer is activated if the fingerprints do not match [8-10]. Four levels make up the security system. Locker security is enhanced by combining various authentication methods. Audio Verification, Password Verification, and Face Verification are the four tiers. By passing through each of the four levels of protection, the user is able to access the protected area [11]. The system reads data from the fingerprint sensor and enters it into the AVR microcontroller, allowing only the authorized user to access the locker and collect the papers or money. Using a simple alert message or buzzer to identify who is entering the locker is not feasible [12]. By securely snapping images using a Raspberry Pi and transmitting them to the user's email address, the deployment of the Internet of Things (IoT) has been carried out, allowing only authorized individuals to access [13]. The ESP32-cam is a well-respected camera sensor that is used for both live streaming and portrait photography. The system is able to identify the person standing in front of the door by using the AI-Thinker in the esp32-2 camera. cited as [14]. The Internet of Things (IoT) gadget is set up to record all activity and will be stored on the cloud. Users' and clients' property is better protected thanks to the Internet of Things (IoT) security system [15]. Several authentication methods are suggested by the system to provide high level security.

II. REQUIREMENTS

A. Arduino UNO

Arduino Uno is a well-liked microcontroller board that offers versatility and user-friendliness in electrical projects. It runs on 5V and accepts input voltages between 7 and 12V, thanks to the Atmega328P microprocessor. Six of the board's digital I/O pins can output pulse width modulation, while the other six can accept analog signals. The 3.3V pin has a current limit of 50 mA, whereas the other digital I/O pins have a limit of 20 mA. There is more than enough memory on the Arduino Uno—32 KB of flash, 2 KB of SRAM, and 1 KB of EEPROM—to store data and code. With a clock speed of 16 MH, the Arduino Uno runs its programs.

B. LCD Display

The performance and usefulness of a Liquid Crystal Display (LCD) are defined by a number of criteria, making it a flexible output device often utilized in electrical applications. Sharper pictures are produced by displays with greater resolutions, which are measured in pixels. LED backlights are widely used because they are brilliant, efficient, and last a long time. Another important factor is the interface compatibility; LCDs may support several interfaces such as I2C, SPI, or parallel communication.

C. Buzzer

A tiny and ubiquitous audio output device in electrical circuits, a buzzer (also called a piezo buzzer) is a typical component. It operates at low voltages, usually about 5V DC, and generates sound by vibrating a piezoelectric element in response to an applied electrical signal. A buzzer's volume may be anything from seventy to one hundred and twenty decibels (dB). When it comes to electronic projects, buzzers are a common way to provide auditory alerts, notifications, or alarms.

D. Node MCU

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Node MCU is a free and open-source platform for the Internet of Things (IoT) that uses the ESP8266 WiFi module. Equipped with a A 32-bit microcontroller from Tensilica, the L106, featuring built-in WIFI and a clock speed of 80 or 160 MHz. For trouble-free wireless networking, the Node MCU is compatible with IEEE 802.11 b/g/n standards. Its general-purpose input/output (GPIO) pins provide for many sensor and actuator interface options, including digital input/output, pulse width modulation (PWM), and I2C, among others.

E. GSM Module

GSM modules provide a variety of characteristics for wireless connection and are hence essential components of communication systems. In most cases, these modules are compatible with a wide range of cellular networks throughout the world since they support numerous frequency bands. The SIM card slots allow subscribers to be identified and authenticated, and they use AT instructions to interface with microcontrollers or other devices. UART ports are often found on GSM modules, allowing for easy communication and integration. Data transmission is protected by authentication and encryption procedures, which are essential components of security. These modules enable efficient energy consumption and run on low power. They provide services such as GPRS (General Packet Radio Service) and SMS (Short Message Service) for data transfer.

F. Servo Motor

When it comes to controlling linear or angular position, servo motors are the way to go. A direct current motor, gears, and a system for providing feedback make them up. The servo can continually change and hold its position thanks to the feedback, which is often a potentiometer. Applications needing controlled movement are well-suited to servo motors due to their reputation for great precision and accuracy. Low voltage is usually sufficient for their operation, and they come in a range of sizes and power levels. Servo motors are controlled via pulse-width modulation (PWM) impulses and have a restricted range of rotation, usually approximately 180 degrees.

G. ESP32- CAM

This development board, the ESP32-CAM, combines the ESP32 microcontroller with a camera module, giving it a strong foundation for Internet of Things (IoT) and image-related applications. It is equipped with WIFI and Bluetooth and uses the ESP32-S processor, which offers dual-core computing. With its 2 megapixels of resolution, the OV2640 camera module may take still photographs or record video. To save media files locally, the board is compatible with microSD cards. A wide variety of sensors and devices may be easily integrated with the ESP32-CAM because to its many interfaces, including GPIO pins, UART, and I2C.

H. Finger print Sensor

Biometric devices that collect and validate unique fingerprint patterns are known as fingerprint sensors. These devices are used for security purposes. In order to get clear pictures of fingerprints, these sensors usually use optical or capacitive scanning technologies. The degree of detail in fingerprint pictures is determined by the specifications of a fingerprint sensor, which include its resolution, which is stated in dots per inch (DPI). One common way to evaluate a sensor's precision is to look at its FAR and FRR.

III. SYSTEM ARCHITECTURE

A. Proposed System

The whole suggested system is shown in Fig. 1, which is a block diagram. By including features such as fingerprint recognition, keypad password input, OTP verification, and real-time picture capturing of unlawful access attempts, the suggested solution aims to improve the security of bank lockers. Secure and easy access is guaranteed via fingerprint recognition, with an additional layer of protection provided by keypad password input. One-time password (OTP) verification reduces the likelihood of unwanted access by creating time-sensitive codes. Integrating

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

IoT devices takes pictures of intrusion attempts and sends them to a manager's bot so that the bot may intervene quickly.

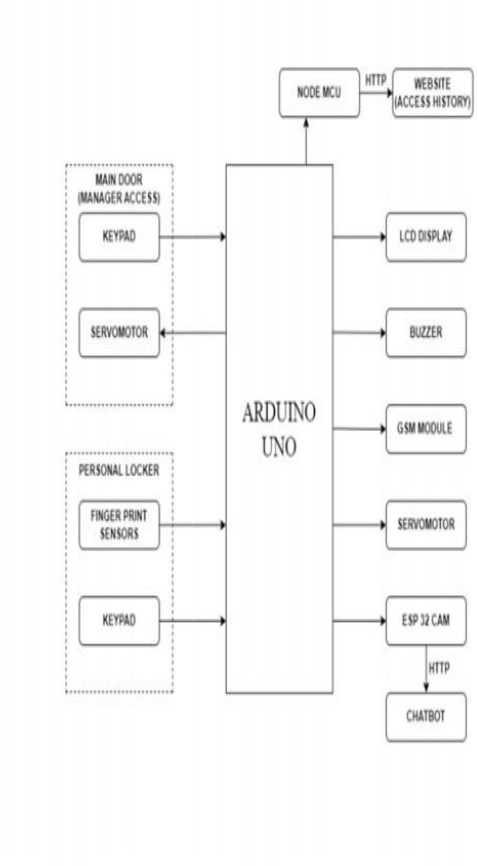


Fig. 1. Block Diagram

B. Process model specification

The proposed system's modes of operation are defined by the process model definition, as shown in Fig. 2.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

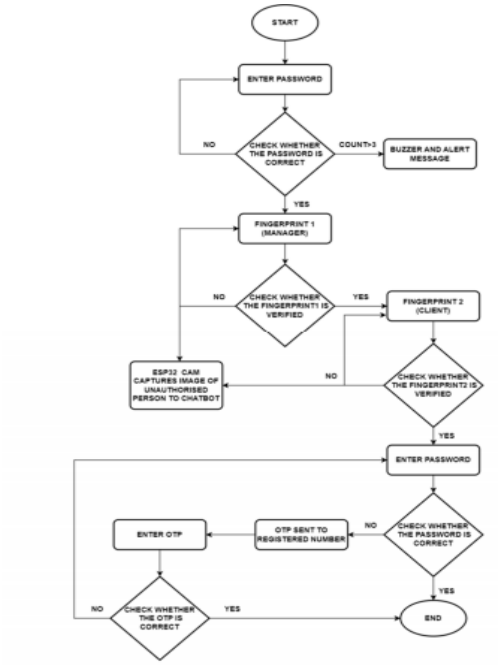


Fig. 2. Flow Chart

IV. PROPOSED WORK

A. Overview

Keeping clients' money and other valuables secure in bank vaults is an area of critical importance for the banking industry. This study introduces a state-of-the-art method for enhancing the security of bank lockers via the use of the Internet of Things (IoT) and several levels of authentication. To provide a strong defense against ever-changing security threats, the suggested solution integrates photo capture in real-time with biometric authentication, keypad password input, and one-time password (OTP) verification.

B. Multi-Layered Authentication System

A complex authentication system, the Multi-Layer Authentication System uses several levels to achieve its goals. Here are the functions and modules they have: 1) Fingerprint Recognition: By taking a picture of a person's fingerprint and studying its distinct characteristics, fingerprint recognition may identify them. The Adafruit Fingerprint Sensor (GT-521F32), which is compatible with Arduino Uno, integrates well with the microcontroller in our suggested solution for bank locker security. Managing the fingerprint sensor's connection to the larger system is a breeze with the help of the Arduino Uno. Through painstaking processing, the inbuilt algorithms in the Arduino Uno locate and extract minute details from the recorded fingerprint data in order to generate a one-of-a-kind fingerprint template. As part of its authentication procedure, the Arduino Uno cleverly checks the recorded fingerprint against pre-stored templates, then either authorizes or denies access according to the verified identity. In addition, the microcontroller uses strong encryption methods to protect sensitive biometric data, which includes

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

fingerprint templates. The bank locker system is made more secure with this integrated solution, which also offers a unique, easy, and dependable authentication technique. 2. Authentication using keypad password: Our upgraded bank locker security system incorporates Keypad Password Entry as a secondary layer of verification after the first fingerprint identification. Users are prompted to enter a unique code using the keypad once their fingerprints have been properly confirmed. The microprocessor of the system, the Arduino Uno, ensures that the keypad and security system communicate with each other without a hitch. Authorized users who have the relevant code may advance to the next level of protection after validating the entered password against stored credentials. To provide another level of security, the lock mechanism of the locker is physically controlled by a servo motor. After the two-factor authentication procedure is finished, the servo motor is activated by the Arduino Uno to lock or open the bank locker, giving a physical and secure way to enter. The addition of a servo motor strengthens the physical barrier, which in turn increases the safety of the bank locker system. Finally, a thorough multi-layered authentication system is put up to safeguard important assets in the bank locker by combining biometric fingerprint identification with keypad password entry and servo motor activation.
Thirdly, we provide an error-handling method that improves the security and user experience of our proposed bank locker security system. An alert message is sent to the client's registered mobile number to advise them of an unauthorized attempt to access their personal locker in the case that the keypad password is entered incorrectly. All the while, a client's mobile device receives an SMS with a randomly created one-time password (OTP). As an additional safeguard, this OTP may be used in place of a traditional password. An LCD display serves as the interface, showing important information such alert messages and one-time password (OTP) prompts, to make interaction smooth. After getting the alert and one-time password, the user is shown on the LCD screen to input the code that they got using the keypad. You will be allowed access to your personal locker if the provided one-time password (OTP) is genuine and matches. This dynamic situation enhances security with multi-factor authentication, makes the bank vault system more user-friendly, and quickly resolves issues caused by wrong keypad entries.

C. IOT integration

1) Capturing images in real-time: A crucial component included into the suggested system to handle any security breaches is the ability to enhance bank locker security via multi-layered authentication and the integration of the internet of things. For example, the system keeps a close eye on password input attempts and initiates a thorough security reaction when it detects three consecutive invalid passwords. This event sets off an ESP32-CAM, an Internet of Things (IoT) camera that is carefully positioned within the bank's locker room. Instantaneously, the ESP32-CAM snaps photos of the intruder in real time. These photos are quickly sent to a manager's chosen Telegram chatbot via the HTTP communication protocol. The authorized manager is able to react and investigate any questionable behavior rapidly because to this well-orchestrated method that provides for immediate visual verification. A proactive protection against possible threats to precious assets housed in bank lockers, this integrated security feature strengthens the entire system's resilience by matching the picture capture process with the occurrence of many unsuccessful password attempts. 2) A complete record of all accesses: The Arduino Uno is the brains of our state-of-the-art bank locker security system, controlling and monitoring everything that goes on behind the scenes. A fingerprint reader is included into the system for user identification. NodeMCU is used for Internet of Things (IoT) connectivity over HTTP. A dedicated website displays dual access history records.In order to confirm the user's identification using biometric data, the Arduino Uno communicates with the fingerprint scanner whenever they try to get access. The entry is recorded in the corresponding access log, whether it's for managers or customers, due to the unique fingerprint signature. The multi-pronged security strategy gains a strong new ally with this biometric authentication. By establishing an HTTP connection between NodeMCU and Arduino Uno, the latter may quickly refresh the website's interface and provide real-time insight into the logs of all accesses. Administrators may keep tabs on permitted access in the main door log, which displays entries made by managers, while customers can see how often their lockers have been used in the client door log.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

V. RESULTS AND DISCUSSION

As shown in the figures below, a well-executed hardware setup is necessary for the effective deployment of the suggested multi-layered authentication system with IoT integration. The security of bank lockers is enhanced by each hardware component, which works together to make the system more durable. Figure 3 shows the hardware configuration, which contains the following components: an Adafruit Fingerprint Sensor (GT-521F32), an Arduino Uno, a keypad, a servo motor, a NodeMCU, an LCD display, and an ESP32-CAM. The capabilities of the Internet of Things (IoT) and the multi-layered authentication system are built upon the smooth integration of these components. The Adafruit Fingerprint Sensor (GT-521F32) and Arduino Uno are used in the fingerprint identification procedure, as shown in Fig. 4. For trustworthy user authentication, the system reliably takes and analyzes fingerprint data. Fingerprints improve the overall reliability and ease of the authentication procedure due to their non-transferable nature and user-friendliness. After fingerprint recognition is successful, users enter a customized code into the keypad, as shown in Fig. 5. When a user presses a key, the Arduino Uno controls a servo motor to make physical access possible. When the user enters the wrong password on the keypad, the process of generating an OTP is shown in Fig 6. For further security, the system may create dynamic one-time passwords (OTPs) and quickly notify the user via their registered cellphone number. Both security and user convenience are enhanced by the dynamic nature of one-time passwords and real-time warnings. Upon detecting several erroneous password attempts, the ESP32-CAM captures real-time photos (Fig. 7). Using the HTTP communication protocol, these photos are sent to a specific manager's Telegram chatbot. An additional layer of preventative protection is provided by the use of IoT for the purpose of real-time picture capture. The system's overall security is enhanced by the quick transmission of pictures, which allows for instant visual verification and response. A dedicated website displays the manager's primary door access record (Fig. 8). The website interface is updated in real-time thanks to the Arduino Uno's communication with NodeMCU over HTTP. The dedicated website displays the client access record (Fig. 9). Thanks to Arduino Uno's ability to communicate with NodeMCU, customers can see their locker usage trends in real time and get fast updates.Users are able to track and examine how they utilize the locker via the client access log. This openness boosts user trust and helps the security system work better as a whole.

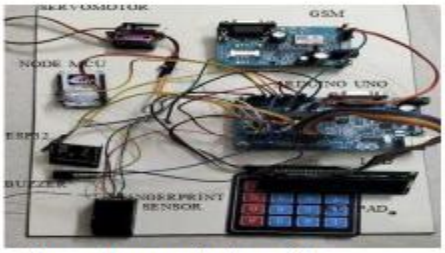


Fig. 3. Proposed system Hardware Setup

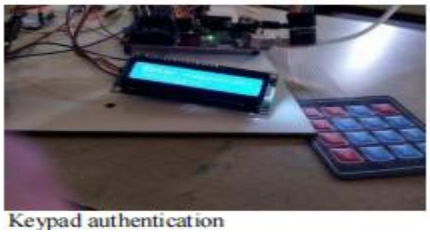


Fig. 4. Keypad authentication

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Fig. 5. Fingerprint authentication

Fig. 6. OTP generation

Fig. 7. ESP32-CAM image captured and sent to chatbot

International journal of basic and applied research

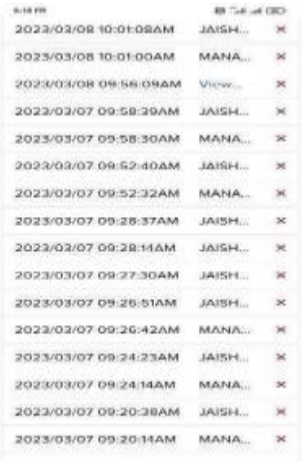
www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Created at	Value
2023/03/13 05:46:28PM	RECE...
2023/03/08 10:00:42AM	RECE...
2023/03/08 09:56:27AM	RECE...
2023/03/08 09:56:06AM	RECE...
2023/03/07 09:56:55AM	RECE...
2023/03/07 09:52:03AM	RECE...
2023/03/07 09:26:24AM	RECE...
2023/03/07 09:22:54AM	RECE...
2023/03/07 09:20:06AM	RECE...
2023/03/07 09:16:28AM	RECE...
2023/03/07 09:13:13AM	RECE...
2023/03/07 09:10:51AM	RECE...
2023/03/07 09:08:48AM	RECE...
2023/03/07 08:59:49AM	RECE...

Fig. 8. Access history log of main door (Manager)



2023/03/08 10:01:08AM	JAISH...	×
2023/03/08 10:01:00AM	MANA...	×
2023/03/08 09:56:09AM	View...	×
2023/03/07 09:58:39AM	JAISH...	×
2023/03/07 09:58:30AM	MANA...	×
2023/03/07 09:52:40AM	JAISH...	×
2023/03/07 09:52:32AM	MANA...	×
2023/03/07 09:28:37AM	JAISH...	×
2023/03/07 09:28:14AM	JAISH...	×
2023/03/07 09:27:30AM	JAISH...	×
2023/03/07 09:26:51AM	JAISH...	×
2023/03/07 09:26:42AM	MANA...	×
2023/03/07 09:24:23AM	JAISH...	×
2023/03/07 09:24:14AM	MANA...	×
2023/03/07 09:20:38AM	JAISH...	×
2023/03/07 09:20:14AM	MANA...	×

Fig. 9. Access history log of personal locker (Manager and client)

VI. CONCLUSION

A multi-layered authentication system that combines the internet of things is proposed, which will significantly improve the security of bank lockers. The system includes a proactive alert system that allows for quick response by combining several authentication methods and using real-time monitoring via the Internet of Things (IoT). It also

strengthens defenses against constantly evolving security threats. Banking vaults are much more secure now that several levels of authentication including fingerprint scanning, keypad password entry, and one-time password verification are all operative. The ability to record and transmit images in real-time via the IoT allows security managers to react swiftly to any attacks. Keeping tabs on who has accessed what allows for improved trend detection and analysis, which in turn helps you find security gaps in your system. The findings of this research will increase customer trust in banks and contribute to the ongoing endeavors to develop better security measures to safeguard monetary assets.

VII. REFERENCES

[1] A.Y. Prabhakar et al., "Password Based Door Lock System" International Research Journal of Engineering and Technology (IRJET), vol 06, issue:02, e-ISSN: 2395-0056, 2019.
[2] J. Baikerikar et al., "Smart Door Locking Mechanism" 4 th Biennial International Conference on Nascent Technologies in Engineering (INCTE), DOI:10.1109/ICNTE51185.2021.9487704, 2021
[3] Arpit Sharma et al., "Smart Locker System" International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), vol02, issue:04, e-ISSN: 2582-5208, 2020.
[4] M. P. L. Chandanshive et al., "Bank Locker Security System based on GSM and RFID", International Journal of Research in Engineering and Science (IJRES), vol. 09, pp.30-33, 2021.
[5] M. Shresta et al., "Bank Locker Security System with 2 Step Verification Using GSM" International Journal for Advanced Research in Science & Technology, vol.12, issue: 11, ISSN: 2457-0362, 2022
[6] S. H. Jadhav et al., "Smart Bank Locker Security System Using Biometric Fingerprint and GSM Technology" International Journal of Science and Research (IJSR), vol.05, issue: 10, ISSN: 2319-7064,
2016.
[7] N. Meenakshi et al., "Arduino Based Smart Fingerprint Authentication System" 1stInternational Conference on Innovations in Information and Communication Technology (ICIICT), DOI: 10.1109/ICIICT1. 2019.B741459, 2019.
[8] K. M. Pooja et al., "Finger Print Based Bank Locker Security System" International Journal of Engineering Research & Technology (IJERT), vol.06, issue: 13, ISSN: 2278-0181, 2018.
[9] L. J. A. Marcilin et al., "Biometric Finger Vein Based Bank Security System Using ARDUINO and GSM Technology" International Journal of Applied Engineering Research (IJAER), vol.13, pp.8774- 8777, 2018.
[10] N.Y.L. Venkata et al., "Intelligent Secure Smart Lock System Using Face Biometrics" International Conference on Recent Trends on Electronics, Information, Communication Technology (RTEICT), vol XIV, Issue: II, ISSN :0022-1945, 2021.
[11] Akash Thomas et al., "Fingerprint Based Bank Locker Security System" International Research Journal of Engineering and Technology (IRJET), vol.08, issue: 07, e-ISSN: 2395-0056, 2021
[12] Saifali Shaikh et al., "Bank Locker System Using IOT Concept" International Journal of Scientific Research & Engineering Trends, vol.07, issue: 02, ISSN: 2395-566X, 2021.
[13] Mohan Kumar et al., "Intelligent Security System for Banking Using Internet of Things" Journal of Computational and Theoretical Nanoscience, DOI: 10.166/jctn.2019.8180, 2019.
[14] Mhaskar et al., "A Survey on IOT Based Secure Bank Locker System" International Journal of Research Publication and Reviews (IJRPR), vol.02, issue: 12, pp 1143-1146, 2021.
[15] Mohan Kumar et al., Intelligent Security System for Banking Using Internet of Things" Journal of Computational and Theoretical Nanoscience, pp 3296-3299, 2019.