Anti Theft GSM Based Digital Bank Locker System With Motion Triggered Capture Technology

Naved Ahmad[1], Shashwat Pandey[1], Shaswat Pandey[1], Amit Kumar[1], Pawan Kumar[1], Pushpendra Kumar Gupta[1,2], Yatindra Gaurav[1]

[1]Department of Electronics Engineering, IERT, Prayagraj-211002, UP, India

[2]Department of Electronics and Communication Engineering, C V Raman Global University, Bhubaneswar, 752054, Odisha, India

***Abstract*-This paper designs and implements a bank locker security system suitable for banks, secured offices, and homes with the help of GSM and motion triggered capture technology. Only authenticated user is allowed to recover assets from bank locker under this system. A security system is developed that activates, authenticates and validates the user identity for secure access to bank lockers. The inclusion of motion triggered capture technology enhances its security even more by real-time image capturing of the user. Image is captured immediately after any motion is detected in the range of PIR sensor. Microcontroller will send OTP to authenticated user's mobile number to open bank locker. After verification the locker will be unlocked if the correct password is entered; otherwise, it will remain locked.**

***Keywords* - GSM modem; microcontroller; ESP32-CAM; PIR**

1. Introduction

In today's society, ensuring safety has become a paramount concern, particularly in both rural and urban areas. Instances of theft and fraud pose significant risks to the security of assets stored in banks, homes, and offices. To deal with these security risks, numerous individuals opt to install several locks or invest in alarm systems. In this project, we present an alternative approach to safeguarding assets stored in bank lockers, homes, and offices by leveraging GSM technology [3]. In this project, individuals do not need to carry identity proofs or keys. This project is based on the OTP generator method, which enhances security. This system will decrease misuse and fraud related to stealing keys, PINs, and ID proofs [4].

This designed system has another feature of capturing image of user by sensing the temperature difference using PIR sensor. The PIR motion sensor continuously monitors its surroundings for any movement. When motion is detected, it sends a signal to the ESP32-CAM, triggering it to wake up from deep sleep mode. Upon receiving the motion detection signal, the ESP32-CAM activates its camera and captures the image of detected motion. The captured image is then saved onto the MicroSD card associated to the ESP32-CAM module and send them via email. ESP32-CAM's deep sleep mode is great for conserving power until it is needed, and using a PIR motion sensor for wake-up signals ensures efficient operation [6].

The rest of the sections are laid out as follows: Literature survey section primarily focused on previous studies similar to this paper. The motivation section tells about idea behind this paper. Approach for presented system section define the working of our system and components used in it. The circuit diagram section defines the pin connections. Comparison section discusses comparative study of existing and presented locker system. Conclusion section provide the benefits of the designed system. Finally, future scope of the presented system is given.

2. Literature Survey

In [1], the idea of door locking system has been presented, a secure door access system using keyless RFID tags for quick and easy unlocking, using passive RFID offers several advantages. Firstly, passive RFID operates without a battery, making it more cost-effective and lightweight compared to active tags. Additionally, a centralized system handles tasks such as controlling, transactions, and operations, streamlining management and ensuring efficient processes. The development of biometric security system using MATLAB simulation gives further idea of identifying people correctly and keeping limited access areas secure [2].

In [3], another approach is made using RFID and GSM, in comparison to other locker systems, passive RFID and GSM based locker system are more secure. This system comprises of microcontroller, RFID reader, GSM modem, keyboard, and LCD, the RFID reader interprets the ID number from the passive tag and delivers it to the microcontroller.

In [4], an enhanced version of GSM is introduced as triband GSM/GPRS. This module featuring an industry-ready interface that is SIM 300 GSM module. In a small form factor, it can send voice, data, and fax using Keil Software (C language).

In [5], the system is designed for detection of the smell patterns of various depositor that are initially stored in the microcontroller. An electronic nose has been developed and is empowered with a software that detects body odors. A variety of sensors can be used to detect odor, including conductivity, piezoelectricity, MOSFETs, optical fibers, and spectrometry.

The security system designed in [6] learns user patterns over time. It stores this information (datasets) on a server at the financial institution. A camera captures the user's pattern (behavior) and sends it for processing. The system then compares this pattern to known patterns and identifies the user if there's a match, before the RFID tag is scanned, the system uses image processing for an initial identification step. This adds another layer of security.

This security setup in [7] comprises four sensors sound, motion sensor, laser, and gas sensor as well as an Internet Protocol camera and a GSM module. The GSM modem is responsible for sending warning SMS alerts to a designated phone number, while the IP camera allows for remote monitoring of the vault room, if any sensor (sound, motion, laser, gas) detects trouble, an alarm blares and a text gets sent to a pre-set phone number. The Arduino (microcontroller) and the GSM (module) make this all happen automatically.

In [8], the process starts with the RFID reader scanning the ID number from the tag and transmitting it to the microcontroller. When a valid ID is detected, the microcontroller sends an SMS request to the authorized person's mobile number, requesting the master password to unlock the bank locker.

This system runs on the ARM 7 (LPC2148) microcontroller, connecting to components like a PC, fingerprint module, GSM modem, LCD, locker, and buzzer. A Java-based interface enables user login, linked to an Apache Derby server and database. During registration, user details such as name, account number, phone number, locker number, and fingerprint ID are stored [9].

In [10], a fingerprint-based bank locker system using ARM7, and GSM technology has been developed. Fingerprint systems offer high security accuracy. The GT-511C3 FPS (fingerprint scanner) is a compact module with an optical sensor on a circuit board. The sensor scans fingerprints, while the microcontroller and software handle the processing automatically.

An IoT-based smart locker with OTP and face detection has been presented in [11] for enhanced security. OTP provides dynamic password security for each login session, while face detection technology ensures authenticity by recognizing human faces in digital images.

A bank locker security system using passive RFID and GSM is presented in [12], which is cost-effective and compact. The system verifies passwords entered via keyboard and mobile phone, opening the locker if correct. An alarm activates if the door is forced to open.

A multi-layer bank locker security system employs RFID cards, biometrics, infrared sensors, and GSM technology is introduced in [13]. Users access the front door with RFID cards and biometric authentication. Infrared sensors detect unauthorized access, triggering alarms and alerts. At the second door, users input locker details and digital signatures for authentication. Robotic arms verify locker validity, granting access upon successful authentication.

In [14], a security system using multifactor authentication like OTP and facial recognition for locker access introduced. Digital lockers offer flexibility by auto-locking after inactivity. Tokens, like RFID chips, ensure secure access. Facial recognition enhances security in locker systems.

Fingerprint recognition technology grants access only to stored fingerprints, even during power failure or battery drain. In [15], multiple fingerprints can be added to include family members or for emergency situations like accidents. The Arduino uno facilitates communication with the R305 module, converting and storing fingerprint data in its database, accommodating over 200 fingerprints.

The GSM-based security system consists a PIR sensor for detect motion through changes in infrared or radiant heat levels. The sensor's output goes high when motion is detected. An IR-based security alarm circuit triggers an alarm upon detecting movement. In [16], the proposed system utilizes the easily available cloud server "thingspeak.com" and an affordable ESP8266 Wi-Fi module.

In [17], web pages are crafted using Python, JavaScript, and SQL, while image recognition relies on Convolutional Neural Networks (CNNs). CNNs are adept at image-related tasks. Haar cascade, another tool, is used for object detection, trained on positive and negative images for accuracy.

In [18], system utilizes a camera, a Raspberry Pi, and a circuit featuring an LCD display with infrared capability for night vision and a USB drive for storage. When the camera detects motion in the video feed, the system employs image processing to identify the exact location of the motion and highlight it. Subsequently, the technology sends photos of the event to the user's computer through IoT. The IoT Gecko platform is utilized in constructing the online system. Additionally, it archives the video footage onto a USB device for future reference. Through the IoT Gecko IoT system, users can decode the online data and view live images of the motion event over the internet.

In [19], a security system was introduced utilizing RFID, password, conveyor, and GSM technologies. This system is designed for banks, secure offices, and homes, ensuring that only authenticated individuals can access and retrieve valuables from the locker. However, the drawback is that if the RFID tag is lost, access to the locker and its contents becomes impossible.

In [20], a microcontroller-based access control system is designed for lockers, with GSM technology. The system's limitation lies in the potential for anyone to access the OTP, compromising its security for the user.

In [21], a new feature to this system is introduced that is the inclusion of a weight threshold sensor, which enhances its functionality. By placing an object on the sensor, the device can measure its weight and

compare it against a preset value. The solenoid lock will only unlock when the weight exceeds the predetermined threshold, ensuring safe access to the locker. This innovative approach effectively decreases the risk of unlicensed access and enhances the overall safety of the system.

In [22], the system incorporates a PIR sensor alongside an ESP32-CAM implanted with IoT technology. Upon detecting motion, the PIR sensor transmits a signal to the ESP32-CAM, prompting it to capture image. Subsequently, leveraging technological advancements, the captured image is wirelessly dispatched to a Telegram messenger app via Wi-Fi. This facilitates monitoring via smartphones or web browsers, presenting a streamlined approach to stay updated with real-time motion events. The effects of delay, parameter uncertainties and nonlinearities for the system are studied in [23-27].

An efficient and budget-friendly security camera system involves leveraging the ESP32-CAM microcontroller along with Blynk (a widely used IoT platform) is designed in [28]. The main goal is to establish a motion-activated surveillance system capable of capturing, storing, and recording video footage, while also providing real-time notifications to the user's mobile device.

3. Motivation

In February 2020, a case came to light, an old couple kept their belongings in the vault. In June 2021, when they opened the locker, they found that it was empty, even the bank does not know what happened. The Reserve Bank of India (RBI) introduced new guidelines effective January 1, 2023, aimed at enhancing the management, transparency, and security of safe deposit lockers in banks. These revisions focus on improving safety, ensuring clear communication, and promoting efficient management of safe deposit services.

In 2024 an article " Are your valuables in bank lockers really safe?" Published in Indian Express which highlights the various problems in bank locker system, like banks typically have CCTV cameras with recording features; however, these are not designed to proactively prevent theft.

In most cases of locker theft, all the financial losses are bear by customer, as banks have not completely insured the lockers and have been lax in compensating victims. Adding to this is the emotional suffering of losing inherited wealth and a connection to one’s ancestry, highlighting the profound trauma that theft victims endure. These incidents and article motivate us to design a secure bank locker system.

The key objective of this paper

The anti-theft GSM based digital bank locker system with motion triggered capture technology is designed to enhance security by verify via OTP and capturing images whenever unauthorized access is detected. This technology can be integrated with Gmail to send captured images and alert notifications directly to your email, ensuring you are promptly informed of any suspicious activity.

1. GSM technology is used to generate OTP for the authorized user. Correct OTP ensures the access of the bank locker whereas, incorrect OTP will trigger the buzzer.
2. The combined use of GSM based locker and motion triggered capture technology enhances the security of the system. This proactive approach ensures that any unauthorized movement within the vicinity of the locker prompts an immediate response, capturing image to identify potential intruders swiftly.

3. The captured image by ESP32-CAM module is saved on MicroSD card also shared via Gmail to user.
4. The overall cost of the presented system is reduced because of use of Arduino nano instead of Arduino uno.

4. Approach for Presented System

The hardware configuration of the system is basically the combination of microcontroller, GSM module, a DC motor, ESP32-CAM and a FTDI module. It also includes a detailed description of the system's overall architecture, functional and nonfunctional requirements.

This system is designed to enhance security by sending alerts and capturing images when unauthorized access is detected. The system is intended to use in commercial as well as residential environments where secure storage is necessary.

4.1. Flow Chart of Bank Locker System

Bank locker system get activated as we press the enter or hast key, the OTP will be sent to the registered mobile number by GSM module. When user types the generated OTP, microcontroller will verify it. If the OTP is correct, lock will be opened; if it is incorrect, buzzer will get activated.

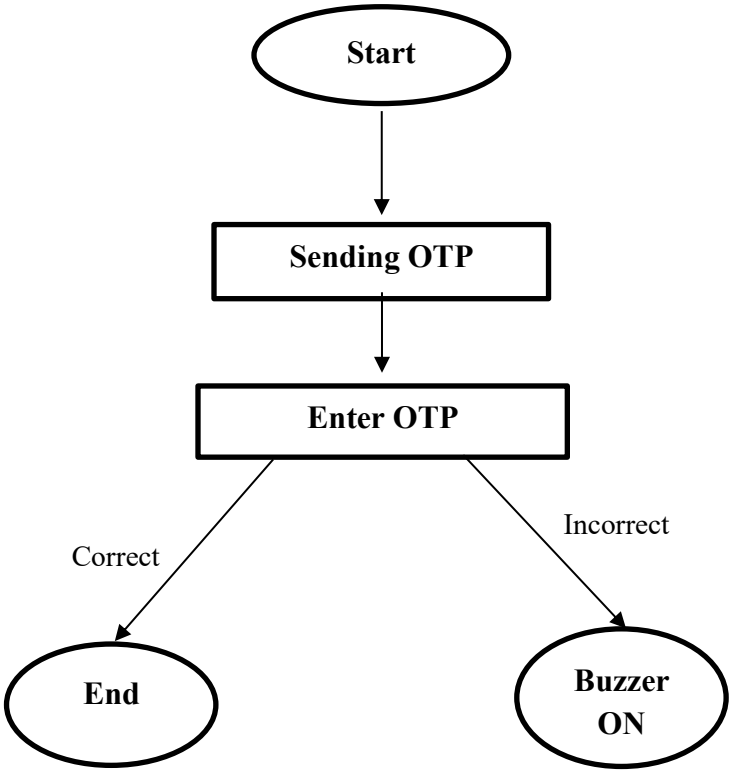

FIGURE 1: Flow Chart of Bank Locker System

4.2. Flow Chart of Motion Triggered Camera

When someone enters in the vicinity of PIR motion sensor, it detects and send an electrical signal to the ESP-32 cam module and it will wake from deep sleep mode. Afterwards, camera module will capture the image and save it to micro-SD as well as send it to registered email id. When there is no motion detected, the whole system will go in deep sleep mode again.

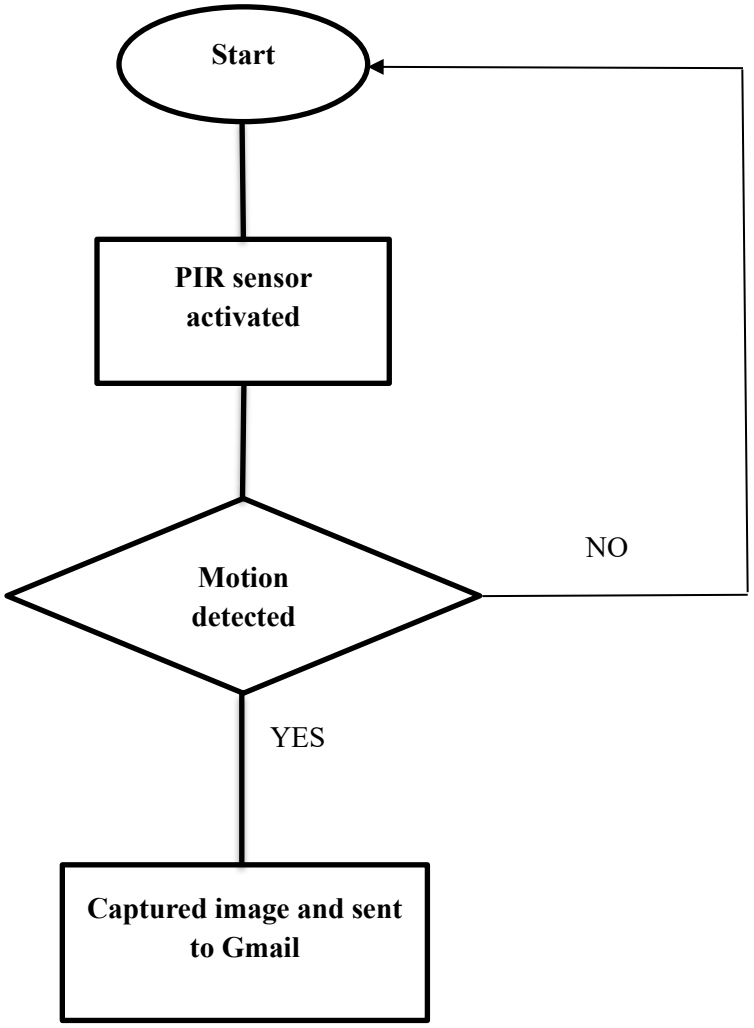

FIGURE 2: Flow Chart for Motion Triggered Camera

4.3. Block Diagrams

The bank locker system is designed around ATmega328p chip. The GSM module send OTP and also communicate with ATmega328p chip, LCD display show the ongoing function like OTP sent, wrong

password etc. Dc motor open the door on instruction of microcontroller. Keypad provides the interface for typing and buzzer will set on whenever the password is wrong.

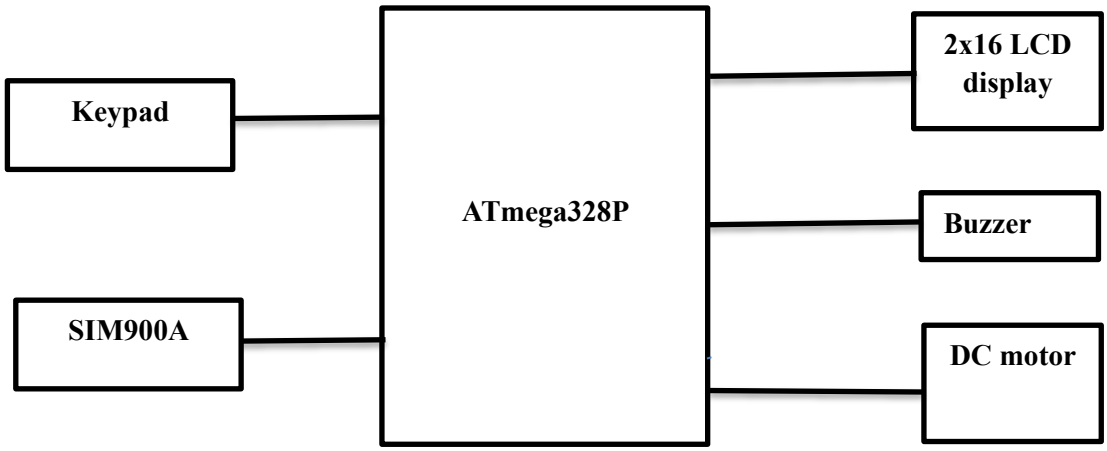

FIGURE 3: Block Diagram of Bank Locker System

The motion triggered capture system is designed around ESP32-CAM module. FTDI programming module provides interface for programming, PIR motion sensor senses the motion around it and ESP32-CAM module captures whenever motion is detected and it also save images as well as send it to registered email.

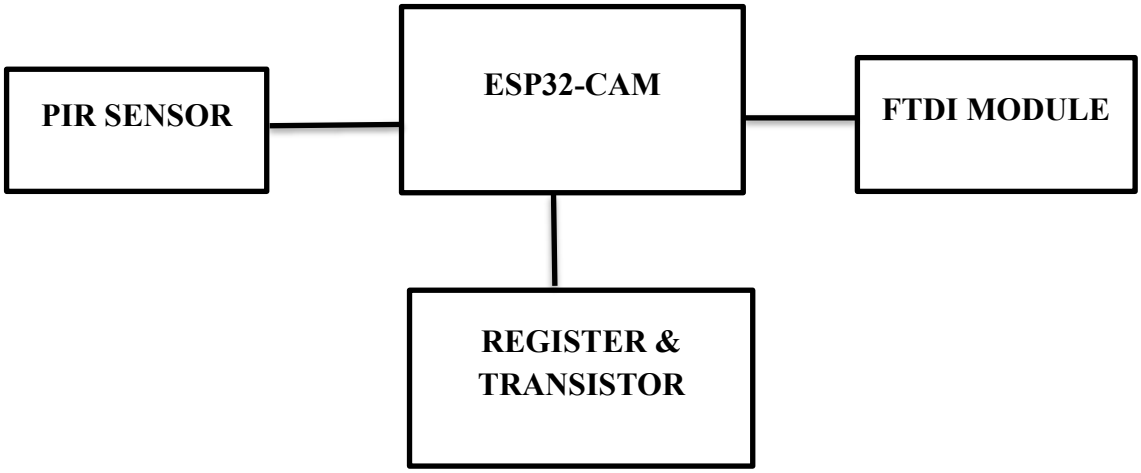

FIGURE 4: Block Diagram of Motion Triggered Camera

5. Circuit Diagram of Presented System

The complete circuit diagram for the Bank locker involves the connection of the GSM module's VCC and GND power supply pins are connected to the Arduino uno's 5V and GND pins. The data pins of the LCD, specifically RS, EN, D4, D5, D6, and D7, are connected to Arduino digital pins 7, 6, 5, 4, 3, and 2, respectively. Additionally, the Rx and Tx pins of the GSM module are directly connected to the Tx and Rx pins of the Arduino.

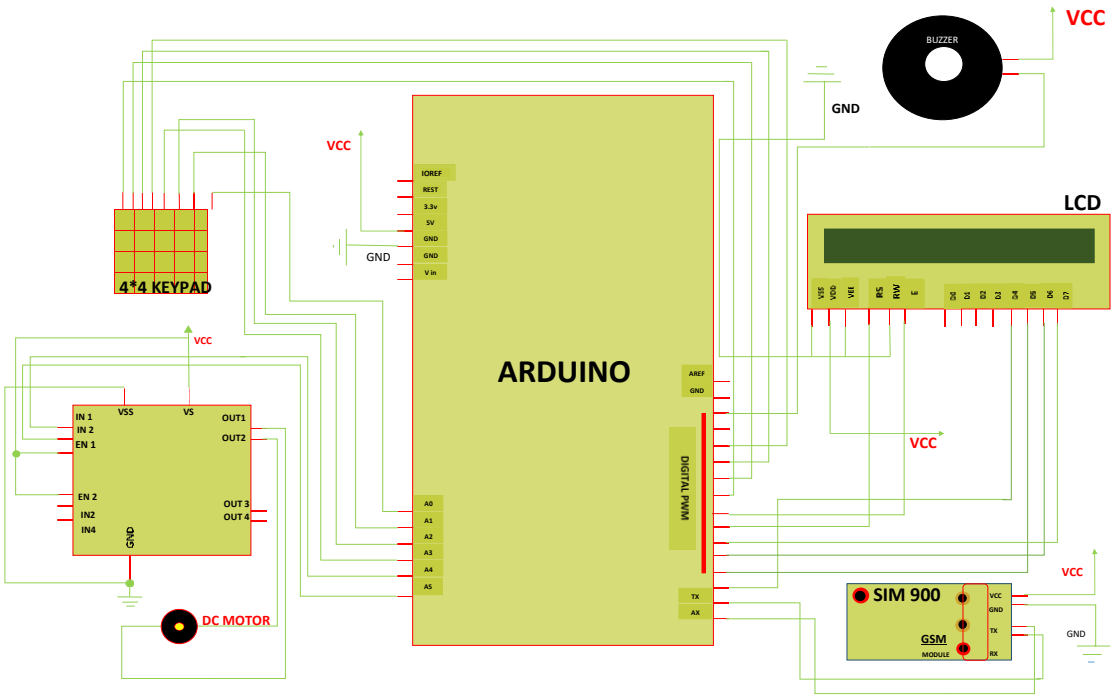

FIGURE 5: Circuit Diagram of Bank Locker System

The circuit for the motion triggered image capture device involves connecting the power pins of the PIR sensor to the 5V and GND pins of the ESP32-CAM. Since the operating voltage of PIR sensor ranges from 4.5V to 12V, so it is connected with the ESP32's 5V pin. The circuit between the motion sensor and the ESP32 generates an interrupt to wake the ESP32-CAM module when motion is detected. To upload code, an FTDI programmer connects to the ESP32-CAM's U0R and U0T (serial) pins. Additionally, the GPIO0 (IO0) pin must be connected to GND to put the ESP32-CAM into flash mode.

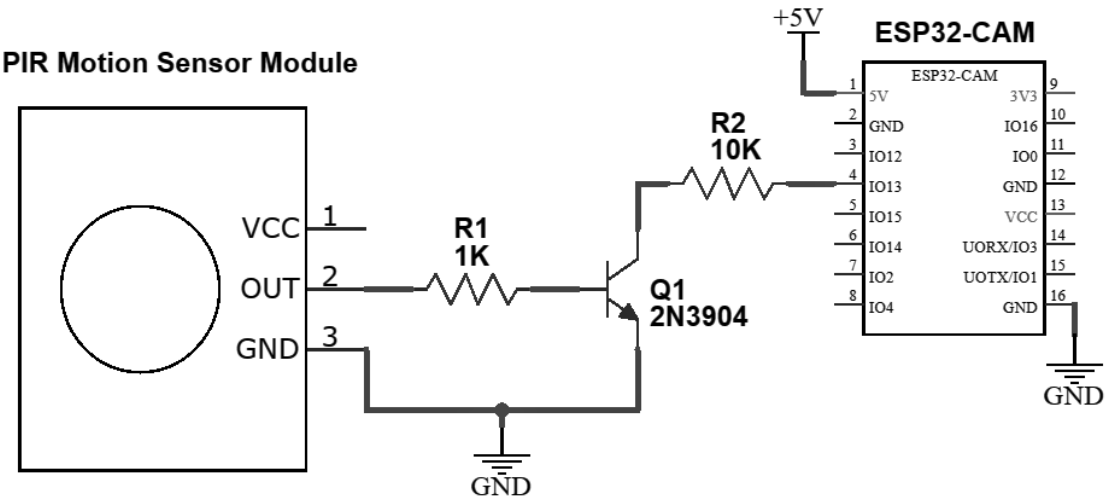

FIGURE 6: Circuit Diagram of Motion Triggered Camera [22]

6. Comparison

The integration of motion triggered camera with existing GSM based locker system is the new approach aims to provide not only real-time alerts but also visual evidence of any intrusion attempts. By comparing the traditional GSM based locker system with the upgraded version incorporating a motion triggered camera, we can evaluate improvements in functionality, security, cost, and user experience. This comparison will help determine the benefits and potential drawbacks of adopting the newer technology in various security applications.

SEQUENCE	TRADITIONAL USED SYSTEM	PRESENTED SYSTEM
1	PASSWORD / ID's & USER	OTP
2	ARDUINO UNO [3,5,16]	ARDUINO NANO
3	WITHOUT MOTION DETECTION TECHNOLOGY [3-8]	WITH MOTION DETECTION TECHNOLOGY
4	WITHOUT IMAGE AUTHENTICATION [9-12]	WITH IMAGE AUTHENTICATION

7. Conclusion

The anti-theft GSM based digital bank locker system with motion triggered capture technology enhances bank lockers security. GSM technology enables real-time monitoring of locker activity, allowing bank staff to track access and detect any suspicious behaviour immediately. It ensures prompt response to security breaches and reduces the risk of theft. Motion triggered capture technology adds an extra layer of security by capturing images whenever motion is detected near the locker area.

8. Future Scope

The presented system when integrated with IoT will provide real-time monitoring and alerts for locker access, ensuring greater transparency and control for users. Implementation of blockchain technology with presented system will ensure transparent record keeping of locker access, enhancing security and trust in the system. The presented system when combined with Aadhar provides another security aspect. The captured image can be matched with UIDAI data, this might reduce the risk of theft and gives complete identification of thief.

References

[1] Verma, G.K. and Tripathi, P., 2010. A digital security system with door lock system using RFID technology. International Journal of Computer Applications, 5(11), p.6-8.

[2] Lourde, M. and Khosla, D., 2010. Fingerprint identification in biometric security systems. International Journal of Computer and Electrical Engineering, 2(5), p.852-855.

[3] Ramani, R., Selvaraju, S., Valarmathy, S. and Niranjan, P., 2012. Bank locker security system based on RFID and GSM technology. International Journal of Computer Applications, 57(18), p.15-20.

[4] Mane, A.D. and Arif, S.M., 2013. Locker security system using RFID and GSM technology. International Journal of Advances in Engineering & Technology, 6(2), p.973-980.

[5] Malhotra, S., 2014. Banking locker system with Odor identification & security question using RFID & GSM Technology. International Journal of Advances in Electronics Engineering, 4(3), p.156-159.

[6] Sugapriya, P. and Amsavalli, K., 2015. Smart banking security system using pattern analyser. International Journal of Innovative Research in Computer and Communication Engineering, 3(8), p.6-15.

[7] Ray, R.K., Uddin, M.A. and Islam, S.F., 2016. GSM based bank vault security system. International Journal of Computer Science and Information Security, 14(2), p.35-37.

[8] Sharma, S., Kumar, M. and Kumar, S., 2016. Bank locker security system based on RFID and GSM technology. Journal of Emerging Technologies and Innovative Research, 3(5), p.66-70.

[9] Malode, S.S. and Patil, S.B., 2017. Advanced security system for bank lockers using biometric and GSM. International Research Journal of Engineering and Technology, 4(12), p.455-459.

[10] Ausekar, P., Kshirsagar, S., Lawate, P. and Inamdar, M.S.A., 2018. Design and implementation of fingerprint-based bank locker system using ARM7 and GSM. International Research Journal of Engineering and Technology, 5(3), p.3038-3042.

[11] Mostakim, N., Sarkar, R.R. and Hossain, M.A., 2019. Smart locker: IoT-based intelligent locker with password protection and face detection approach. International Journal of Wireless and Microwave Technologies, 9(3), p.1-10.

[12] Chintam, S. and Venkanna, B., 2019. Bank locker security system with password and intruder alarm. International Journal for Recent Development in Science and Technology, 3(1), p.72-77.

[13] Islam, M.A., Sarder, M.S., Mamun, M.H., Ahmed, F., Sarkar, S.K., Mridul, A.H, Ahmed, M.T. and Khatun, T., 2022. Multi level bank locker security system with digital signature authentication and IoT. Research square, p.1-15.

[14] Dhoot, A, Shumka, K., Saeed, M.S., and Nazarov, A.N., 2021. Multi factor authenticated secure digital locker using GSM. Synchroinfo Journal, p.7-12.

[15] Shreshta, M., Bhavana, P., Manasa, P. and Kumar, G.H., 2022. Bank locker security system with 2 step verifications using GSM. International Journal of Advanced Research in Science and Technology, 12(11), p.73-79.

[16] Pooja, K.M., Chandrakala, K.G., Nikhitha, M.A., & Anushree, P.N., 2018. Fingerprint-based bank locker security system. International Journal of Engineering Research and Technology, 6(13), p.1-5.

[17] Vishwakarma, M., Gite, R., Katyare, B., Kokane, P. and Sabale, R.P., 2018. Bank locker protection with liveness detection using machine learning. International Research Journal of Modernization in Engineering Technology and Science, 4(11), p.352-357.

[18] Kshirsagar, P.R., Akhtar, F., Ikhar, A.K. and Chaurasia, K.S., 2012. IoT-based theft detection using raspberry pi. International Journal of Food and Nutritional Sciences,10(2), p.500-506.

[19] Soares, J. and Gaikwad, A.N., 2016. A self-banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP. International Conference on Communication and Signal Processing, p.0508-0512.

[20] Joshi, P. C. K.N., 2018. A survey of cancellable biometric based key generation scheme using various cryptography techniques. International Journal of Computer Sciences and Engineering, 6(3), p.1-6.

[21] Naukarkar, V., Waghade, N., Dukale, S. and Patil, S.S., 2023. Bank locker system using fingerprint, OTP and threshold weight. Journal of University of Shanghai for Science and Technology, 25(6), p.78-91.

[22] Yunus, N.H.M., Zamri, M.I.M. and Yusof, N., 2024. Development of a motion activated security cam for monitoring applications. In Applied Problems Solved by Information Technology and Software, p.1-8.

[23] Gupta, P. K., Singh, K., Kandanvli, V. K. R. and Kar, H., 2023. *New Criterion for the Stability of Discrete-Time Systems with State Saturation and Time-Varying Delay*. Journal of Control, Automation and Electrical Systems, 34(4), pp.700-708.

[24] Gupta, P. K. and Kandanvli, V. K. R., 2020. New LMI criteria to the global asymptotic stability of uncertain discrete-time systems with time delay and generalized overflow nonlinearities. In Advances in VLSI, Communication, and Signal Processing, Springer, pp. 883-895.

[25] Gupta, P. K., Singh, K. and Kandanvli, V. K. R., 2022. Further results on delay-dependent stability analysis of uncertain discrete-time systems exerting generalized overflow nonlinearities and time-varying delays. In Recent Trends in Electronics and Communication, Springer, pp. 1081-1100.

[26] Gupta, P.K. and Kandanvli, V.K.R., 2024. Delay-dependent LMI condition to the stability of a category of uncertain discrete-time systems exerting quantization/overflow nonlinearities and variable time-lags. Journal of Systems Engineering and Electronics. 34(4). pp. 150-161.

[27] Gupta, P.K., Singh, K. and Kandanvli, V.K.R., 2020. Further LMI conditions to the stability of the delayed discrete-time systems subject to generalized overflow nonlinearities and parameter uncertainties. In 7th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). pp. 1-6.

[28] Patil, A., Pati, S., Momin, L., Patil, Y. and Nalawade, S.,2023. ESP32-CAM motion sensor security camera with notification using blynk. International Research Journal of Modernization in Engineering Technology and Science, 5(12), p.353-356.