AOI: 10.11234.2024.00032
ACT2024: Special Proceedings of Applied Computer Technology

RFID and GSM Based Bank Locker Security System With Enhanced Authentication

Suman Chakraborty[1], Sandipan Patra[1], Sudeshna Nath[1], Suhas Deb[2]

[1]Electrical Engineering Department, Budge Budge Institute of Technology,
Nishchintapur, Budge Budge, West Bengal, India
[2]Electrical Engineering Department, Hooghly Engineering & Technology College, Hooghly, West Bengal, India
Corresponding author: sandipanpatra2001@gmail.com,

ABSTRACT

In the upcoming era, security is going to be a vital factor for emerging conventional and stereotypical society. This refers to the higher risk management which needs to be supervised by the higher authority in the government sector as well as in the banking field ensuring improvement in the safety measurement and technical development. However, the main concern should be focusing on implementation of an acquainted and desirable model which will not only protect individual's accessories to get cheated from fraudulent but also incorporate the tangible durability and intellectual property. The predominant motive of this designed module is to demonstrate a secure bank locker system employing RFID and GSM for enhanced protection along with some beneficial topologies. It will decrease time consumption for both bank authority as well as its associated locker holders comprised with suitable mechanism which adheres only the genuine person to get access to the bank locker inscribed against particular name.

As per nomenclature of the prototype, the system consists of different RFID oriented elements having operated current of 13-26mA per 3.3V DC and specialization in 13.56 MHz non-voice contact & GSM modem having input voltage range from 3.4V to 4.5V with certain and adjustable data transmitting and receiving speed. These two components are generally automated by ATmega328P based microcontroller. In this regard it should be conveyed that this microcontroller operated system incorporates some extra ordinary features providing flexible and smoother locker access but cultivating advanced technical strategy and well defined methodologies. Coming into the operational aspect, the researched work includes the use of two credential IDs (Customer ID & Locker ID), registered contact number and RFID encrypted ATM card. If the user enters all credentials correctly with having proper data, then normally a four-digit numeric code will be created to the immediate account holder's phone utilizing GSM module and finally the locker door will be unlocked, otherwise the system will get coupled with the help of servo motor mechanism and an buzzer will flow consequently on every prompt and appropriate verification.

Keywords: Atmega328P Microcontroller, RFID Tag & Reader, Unique Identification Codes (GSM SIM 900), OTP generation, LCD Screen, Buzzer, Electrically Operating Vault.

I. INTRODUCTION

Our designed system is able to restrict the unauthorized intrusion and it will assist to reduce fraud scheme to banking locker system so that each and every customer adequately ensures their property security under the surveillance of banking authority [1]. As the account hacking is being increased through online media day by day and many old aged persons are unaware about the money hacking process due to their lack of knowledge regarding advanced technology, therefore in order to protect them from being cheated this system is mainly designed [2]. In the other hands, the composite module will restrain the human intervention extensively which makes it enable to restrict time consumption as well as reduces involvement of manpower. Consequently, no extra salary or remuneration and other benefits provided to the banking employees need to be bothered by any banking sector for assigning this particular task. Therefore, the proposed system facilitates entire operation economically and technically enhancing the overall performance, accuracy and efficiency of the arrangement. Along with ensuring the safety of the bank locker, the system also alerts staff members to recognize the unauthorized individual. This indicates that the system offers dual functionality, ensuring the security of banking lockers and enabling proactive detection and response to criminal activities [3]. With these cumulative and creative natures of the prototype, we preferably Bank Employee

from different branches can effortlessly attain the maximum rate of customer from various regions. This ultimate arrangement allows every banking regions to maintain appropriate time frame addressing to each and every associated customers at a suitable time interval. This system consists of three security steps which will allow only the authorized person (customer) to access the locker belonging to him only. Additionally, taking into account all the safety & precautions of the banking rules and regulations, the system's configuration is made to support flexible and seamless adaptation by the old aged and physically challenged locker holders. More precisely, it highlights the multi-layered approach which ensures comprehensive protection and peace of mind for all users particularly those who are less tech-savvy and more vulnerable to fraud [4].

The subsequent sections of the work are structured as follows: Section-I describes the key principal of this work, Section-II implies the necessity and actual overview of this researched work, Section-III comprises of various literature work regarding this paper, Section-IV provides actual system design strategy and every component functionality of this module, Section-V contains operational output of the proposed prototype and the last but not the list conclusion & future development part are depicted in the Section-VI.

II. LITERATURE REVIEW

A. Smart locker bank design optimization for urban Omni channel logistics:

In this paper two most popular authors namely videlicet Louis Faugère, Senior Applied Scientist at Amazon and Georgia Institute of Technology & Benoit Montreuil, Professor ISyE, Georgia Tech: Executive Director Supply Chain & Logistics Institute, Director Physical Internet Centre, Coca-Cola Chair Material Handling & Distribution Atlanta, Georgia, United States, depicts the optimization related developed instances for smart locker bank in which they proposed two authenticated approaches, furnishing empirical substantiation of their performance and relating avenues for future exploration. Smart lockers are automated, secure storage units designed for essential item storage, accessible 24/7 through smart authentication methods such as government-issued IDs or smartphones. Deploying networks of smart locker systems offers potential benefits, including reduced delivery costs, decreased urban traffic congestion, and lower greenhouse gas emissions. However, challenges associated with the deployment and operation of such networks have been primarily explored through empirical analysis, simulation modelling, and industry based observations. Despite this, limited research has focused on the structural design and implementation of smart locker banks. This design challenge is particularly significant in densely populated metropolitan areas, where real estate is both expensive and limited. Therefore, it is crucial to develop effective design strategies for smart locker systems to ensure optimal space utilization and enhanced customer satisfaction.

B. Design of a privacy-preserving cloud locker utilizing Paillier encryption and chaotic cryptography techniques:

In this paper, the authors namely Vinod Ramesh Falmari, Lecturer of the Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, India & M. Brindha, Associate Professor of the Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, India combinely proposed and developed a cloud oriented digital image locker system using fixed user authentication and novel image cryptosystem for conserving privacy of user photos. The cloud system following specific protocol is used to trace and analyse the user's personal images and data stored in a database to get important information which will be hidden from public gallery. A cloud storage service based technology can also be best solution for preserving user's authentic documents or certificates such as driving licences, government issued ID card, academic mark list, property and legal papers and many more. The proposed authentication protocol is formulated with the help of Paillier based difference function which is defined on Homomorphic cryptosystem. The advantage of using homomorphic function is that computation on encrypted data is feasible without decrypting the cipher text. An image processing cryptosystem is designed using the concept of Fridrich model. Functional keys are modified in each round of confusion to achieve more reliability.

C. A Biometric and GSM-Enabled Smart Security Framework for Bank Lockers:

In this study, Subhash H. Jadhav and S. S. Agrawal-Associate Professors from the Department of Electronics and Telecommunication at Government College of Engineering, Dr. B.A.M. University, Aurangabad, India present a structured and comprehensive paper on a smart bank locker security system. The system integrates RFID, password authentication, GSM communication, and biometric fingerprint verification to enhance security. Their approach ensures that only authenticated individuals can access the locker to retrieve valuables such as important documents, jewellery, or cash. Within the proposed framework, they incorporate two verification steps from which one of them is enrolment process of every user by entering correct username, password and mobile number and then users have to put their finger on Fingerprint module which detects and stores the actual Fingerprint ID and another one is locker accessing procedure for which user has to swipe RFID tag on RFID reader and then again correct fingerprint data should be fetched from the stored database which allows the user to enter actual password. During this verification process if any data mismatches then this system will generate alarm bell and notify the user by showing a

warning message. However, they also activate the siren horn in the system during every successful operation. In these whole functionality, every credentials need to be operated confidentially which ensure reliability and safety of the system from fraudulent. Although it will be time consuming and lengthier process whether it is executed via online or offline.

III. SYSTEM DESIGN:

3.1 Component Operational Features:

1. Arduino UNO : Arduino UNO is an open-source device which plays crucial role in handling all electronic software and hardware based projects. In this prototype, all input commands needed for entire execution are encoded into it which will be turned into output as displaying welcome message, identifying and verifying user's credentials, activating GSM for OTP generation and so on.

2. RFID MFRC 522: It is a highly integrated RFID Card Reader which can able to work on 13.56 MHz contactless communication. In this module it work as an interpreter i.e. it analyzes electronic data and then make readable for the system to provide contactless communication.

3. RFID Tag: It is mainly defined as Radio Frequency Identification (RFID) electronic tag which interchanges encoded data with machine level data using radio waves to be read by RFID Card Reader for execution.

4. GSM SIM 900: GSM modem is nothing but a tele-communicating device which transmits and receives mobile signals using GPRS (General Packet Radio Service) Protocol. In this prototype, GSM modem is used to create authenticated code via cellular 3G or 4G networks (OTP) against registered mobile no. after getting input command from Arduino UNO.

5. Servo Motor: It is also called rotary or linear actuator which helps to precisely control the angular or linear position of any object (remote-controlled toys, automatic doors, cameras etc.) associated with built-in feedback mechanism. In this designed model, it is used to monitor and actuate the angular position of the locker door based on specific time period.

6. Buzzer: Buzzer or Beeper is an audio signaling device which can be mechanical, electromechanical or piezoelectric. Here it is associated with Arduino UNO element to make a beeper sound on every appropriate function of the module.

***7. I2C LCD Display*:** It's an output device which is used to display 16 characters in white colour on 2 rows in blue background at a time based on the user input. In this system this display is able to visualize every step wise operation on the screen receiving input command from the Arduino UNO processor.

8. Keypad: This is nothing but a pad or block of patterns with a set of arrangement containing alphabetical letters, special symbols and numeric keys. Here it will be used to provide the input credentials by the respective account holders which actuates the processor to generate outputs.

3.2 Circuit Component List:

Table-1 is appended at end of the paper which contains circuits components as APPENDIX-1

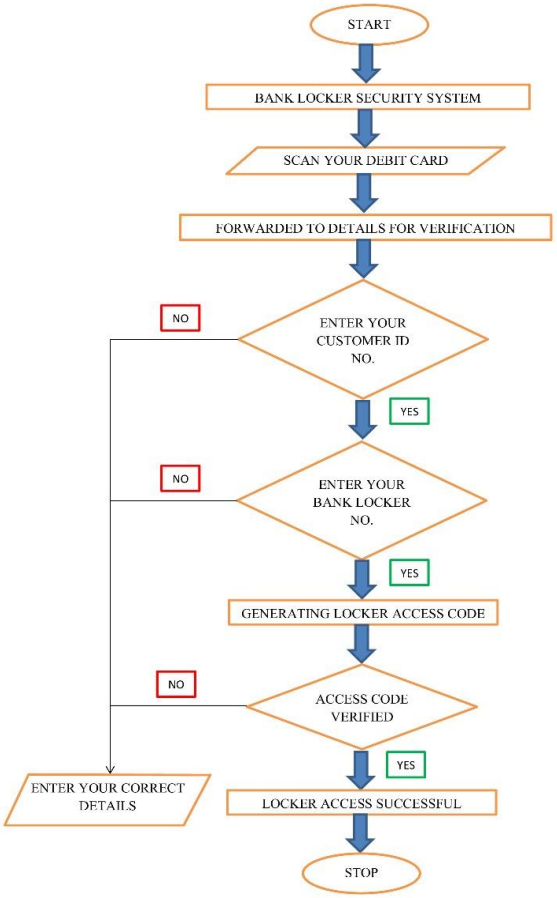


Fig-1. Flow Chart for the Designed model

Fig.1. shows the operating layout of our designed system. The above mentioned flow chat describes that at first the system will be switched on and it will display welcome message. Now the user has to scan his RFID enabled card which will carry forwarded to the next authentic steps i.e. Customer ID and Bank Locker ID need to be entered by the account holder correctly otherwise the process will be repeated on continuous basis until and unless the prototype receives the actual credentials of the user. After getting correct data from the account holder, a four digit access code will be generated on the registered mobile number of the authenticated user which will be entered by the user properly for verification purpose in order to avoid resetting entire process. Finally based on the successful operation of every steps, the locker will be unlocked and

it will remain open for certain period of time to get enhanced protection.

3.3 Working Principle:

#Step 1:

At first, power supply is provided to the prototype using 12V DC Power Supply and the procedure starts when Arduino UNO of ATmega328P Microcontroller will ask to generate command in the module that will be displaying a welcome message.

After displaying message, we need to scan RFID enabled card which is detected through RFID electronic tag and it exchanges encoded electronic data with the machine level language using radio waves which are read by RFID MFRC 522 card reader and then associated command will ask for Customer ID number and if account holder do any mistake to enter the Customer ID number, then the In-build process will be continued within a closed loop and it will ask to re-enter the customer ID at every wrong attempt, otherwise the user has to reset the system.

#Step 2:

If the Customer ID number entered by user tallies with the stored database of the system, then only Buzzer will blow which indicates account holder can proceed to next step i.e. user has to enter Bank Locker No.

Just like in the previous step, If there is any mistake in typing the Locker no. by the user then this system will permit the account holder to reenter the Locker no. and if the user fails to do so again then the continuous closed loop will not allow to proceed next step and ask for same in each case otherwise the system has to be reset. But in the other provision of putting actual Bank Locker No., Buzzer generates a beeper sound and the system

Fig-2. Front View of Designed Model

operation will be forwarded to next step.

#Step 3:

After the successful execution of above-mentioned steps, Locker access code will be generated via GSM SIM900 module to the registered mobile no. of the account holder which is already stored in the database of the system.

After receiving this access code, the account holder has to enter it properly. If the user fails to enter the code correctly, then the process will repeat iteratively by showing the message in the display “enter again”, otherwise on the eminent verification of the access code, the buzzer will make a sound and the locker door will be opened using servo motor operation for restricted time period.

3.4 Model Demonstration:

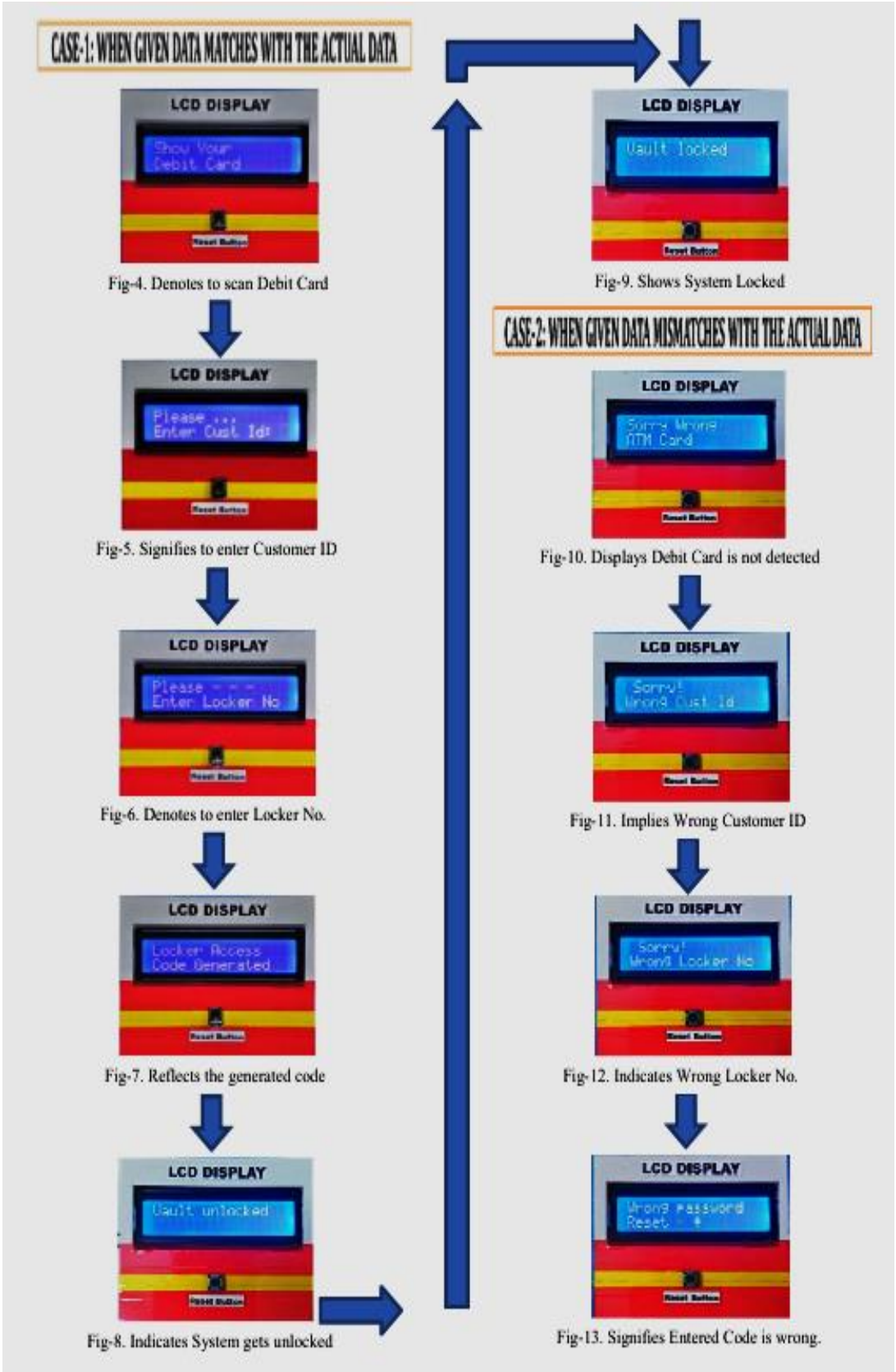
Fig-3. Side View of Designed Model showing different elements

IV. OUTCOMES AND DECISION:

4.1 Explanation & Pictures of Implemented Module under Operating Condition:

The below mentioned figures No. from “4” to “9” for CASE-1 are depicted in the below as:

- **Fig-4:** It implies to scan the RFID enabled Debit card.
- **Fig-5:** It indicates to enter the user associated Customer ID No.
- **Fig-6:** The system asks to enter the user registered Bank Locker No.
- **Fig-7:** 4 digit Access Code will be generated based on registered credentials.
- **Fig-8:** Locker door will be unlocked after appropriate verification of all functionalities.
- **Fig-9:** Locker door will be locked automatically after couple of times to secure and protect the system.


CASE-1: WHEN GIVEN DATA MATCHES WITH THE ACTUAL DATA
LCD DISPLAY
Show Your Debit Card
Fig-4. Denotes to scan Debit Card
LCD DISPLAY
Please ... Enter Cust Id:
Fig-5. Signifies to enter Customer ID
LCD DISPLAY
Please - - - - Enter Locker No
Fig-6. Denotes to enter Locker No.
LCD DISPLAY
Locker Access Code Generated
Fig-7. Reflects the generated code
LCD DISPLAY
Vault unlocked
Fig-8. Indicates System gets unlocked
LCD DISPLAY
Vault locked
Fig-9. Shows System Locked
CASE-2: WHEN GIVEN DATA MISMATCHES WITH THE ACTUAL DATA
LCD DISPLAY
Sorry Wrong ATM Card
Fig-10. Displays Debit Card is not detected
LCD DISPLAY
Sorry! Wrong Cust Id
Fig-11. Implies Wrong Customer ID
LCD DISPLAY
Sorry! Wrong Locker No
Fig-12. Indicates Wrong Locker No.
LCD DISPLAY
Wrong Password Reset - *
Fig-13. Signifies Entered Code is wrong.

The below mentioned figures No. from "10" to "13" for CASE-2 are depicted in the below as:

- **Fig-10:** It implies that associated Debit Card is not identified. So actual ATM card should be detected otherwise it will display the same and cannot allow to move next step.
- **Fig-11:** It indicates that entered Customer ID No. does not match with the actual one. Until and unless correct Customer ID is given it will display the same and hold it to present step.
- **Fig-12:** It signifies registered Locker ID No. is not correct input. So without providing genuine ID No. the system will be stick in the same phase.
- **Fig-13:** It means Locker Access Code does not satisfy. Eventually in this stage also, entering wrong OTP by the user will interrupt to access the locker.

Please Note, every wrong input at each step given by the user are not associated with each other so any wrong data entered by the locker holder at any step will be terminated in the current stage where the user actually left and therefore the system are to be reset for smooth starting.

Depending upon the final implementation of the above model, we will be getting smooth and reliable services under the strong surveillance of bank authority. As the designed prototype comprises of multiple steps to access the locker so it will be allowing only the actual and genuine customer of the respective locker. With the help of this system we will be able to identify the fraudulent individual easily in case of any mismatch while putting the details.

V. CONCLUSION & FUTURE DEVELOPMENT:

The RFID & GSM-based bank locker security system tributes fundamentally to in enhancing the safety and confidentiality of valuables in monetary institutions. By integrating advanced technologies, strict access controls, and proactive monitoring, these systems effectively prevent threats such as theft, unauthorized entry, and environmental risks. Designed with essential security features, the system ensures reliability while prioritizing customer satisfaction, thereby reinforcing its stability. The implementation of a two-step verification process enhances security by minimizing unauthorized access, making it highly efficient and well-organized. As technological advancements continue, these systems will further evolve, strengthening security measures and maintaining the integrity of banking services. Analyzing different aspects and terminology of various author's manifestation it is observed that the proposed prototype will contribute more productive and beneficial result than other predefined system to make sure positive feedback from the account holder and thereby this type of immutable and stabilized system will be sustainable enough to fulfill the customer's requirements and expectations.

Future enhancements will focus on improving the prototype's efficiency and functionality by incorporating stricter security measures. For instance, physically challenged individuals relying on others for locker access may face risks if the entrusted person has malicious intent. A notification system via mail or text can alert the owner about locker usage, enhancing security. Additionally, unrestricted access attempts can pose risks, making it necessary to impose limitations to ensure smooth and secure operations for all users.

ACKNOWLEDGEMENT

This document is made with the help of Applied Computer Technology, a research oriented technology based company. Along with that, I would like to express my sincere gratitude to my supervisor, Ms. Sudeshna Nath, for her amicable guidance, relentless encouragement and continuous feedback throughout the entire process of this research. Her wisdom and valuable thoughts have tremendously supported me to achieve final goal of this research work.

I am also thankful to my colleagues and peers who imparted me lots of significant and informative resources which makes this work more productive and beneficial.

Finally, I am deeply grateful to my co-authors for their immense enthusiasm, perseverance and coordination to accomplish the research activity.

REFERENCES

[1] SD Kaul and D. Hatzinakos, "Intelligent RFID biometric enabled dual security lock in the banking environment", Journal of Banking and Financial Technology, vol. 4, pp. 159-173, September 2020.

[2] 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.

[3] Gyanendra K Verma, Pawan Tripathi, "A Digital Security System with Door Lock System Using RFID Technology", International Journal of Computer Applications (IJCA) (0975 – 8887), Volume 5– No.11, August 2010.

[4] Pravada P. Wankhade1 and Prof. S.O. Dahad2, "Real Time Vehicle Locking and Tracking System using GSM and GPS Technology-An Anti-theft System", International Journal of Technology And Engineering System(IJTES), Jan –March 2011- Vol.2.-No.3.

[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, no. 11, pp. 2457-0362, 2022.

[6] M. S. Divya and M. N. Rao, "Centralized Authentication Smart Locking System using RFID, Fingerprint, Password and GSM", International Journal of Engineering & Technology, vol. 7, no. 3.12, pp. 516–520, Jul. 2018.

[7] Li, B., Chen, R. S., & Wang, H. C. (2021). Using intelligent prediction machine and dynamic workflow for banking customer satisfaction in IoT environment. Journal of Ambient Intelligence and Humanized Computing, 1–10.

[8] Deeksha P, Mangala Gowri MK, Sateesh R, Yashaswini M, Ashika VB (2021) OTP based locking system using IOT. Int J Res Publ Rev 2(7).

[9] X. Huo et al., "Intelligent electronic passworded locker with unique and personalized security barriers for home security", Nano Research, vol. 16, no. 5, pp. 7568–7574, May 2023.

[10] Sonali Lunawat et al., "3-Level Authentication for Bank Locker Security", International Journal of Scientific Research in Multidisciplinary Studies, vol. 5, no. 6, pp. 44-47, June 2019.

[11] N. N. San Hlaing and S. San Lwin, "Electronic Door Lock using RFID and Password Based on Arduino", International Journal of Trend in Scientific Research and Development, vol. 3, no. 2, pp. 799-802, 2019.

[12] H. F. Alqahtani, J. A. Albuainain, B. G. Almutiri, S. K. Alansari, Ghaliah B. AL-awwad, N. N. Alqahtani, et al., "Automated Smart Locker for College", 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 2020.

[13] C. Munoz-Ausecha, J. Ruiz-Rosero and G. Ramirez-Gonzalez, "Rfid applications and security review", Computation, vol. 9, no. 6. MDPI AG, Jun. 2021.

[14] Ripan Kumar Ray, M. A. U. S. F. I., February 2016. GSM Based Bank Vault Security System. International Journal of Computer Science and Information Security (IJCSIS), 14(2), pp. 35-38.

APPENDIX-1:

Table-1: circuit components values.

SL.	Components	Specification and Cost in INR
1	Arduino UNO	Microcontroller: ATmega328P, Input Voltage: 7-12V, Digital I/O Pins: 14, PWM Digital I/O Pins: 6, Clock Speed: 16MHz (415 INR)
2	RFID MFRC 522	Frequency: 13.56MHz (91 INR)
3	RFID Tag	13.56 MHz (200 INR)
4	GSM SIM 900	Voltage: 3.4V-4.5V, Serial Baud Rate: 1200-115200 bps (300 INR)
5	I2C LCD 16*2 Display	Voltage: 5V DC +/-0.5V (350 INR)
6	Buzzer	Voltage: 4~8V (25 INR)
7	Keypad	As per requirement
8	Servo Motor	I/P Voltage: 5V (250 INR)
9	Flexible Wires	As per requirement
10	Adaptor	12V, 3 Pin (130 INR)
11	Solder iron	48Watt (250 INR)
12	PCB	As per circuit requirement.

Cite this article as:

Suman Chakraborty, Sandipan and et.al. "RFID and GSM Based Bank Locker Security System With Enhanced Authentication", ACT2024: Special Proceedings of Applied Computer Technology, Published in August 2025, Link: http://actsoft.org/science/act2024-pro/86-micro2025.pdf , AOI: 10.11234.2024.00032

Website: actsoft.org, Email: info@actsoft.org, published on: August 2025. ISBN: 978-81-985770-3-0