



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 5, May 2017

Wireless Communication Locker with Advanced Security System using GSM, RFID and OTP Technology

Prutha Suroshi¹, Radhika Hambire², Priteshsingh Chandel³, Milana Malvadkar⁴

B.E. Students, Dept. of C.S., P.E.S MCOE, Savitribai Phule Pune University, Maharashtra, India^{1,2,3}

Assistant Professor, Dept. of C.S., P.E.S MCOE, Savitribai Phule Pune University, Maharashtra, India⁴

ABSTRACT: The main purpose of this paper is to design and implement advanced locker security system. In today's materialistic world, security holds in dispensable place. There is need of security in almost every sector of society such as offices, banks, and houses etc. as thefts and robberies increasing day by day. To overcome this security threat, a security system has been proposed using Controller and GSM Technology. This system is basically a controller based access control system which allows only authorized person to access the locker with GSM technology. This system activates, authenticates and validates the user and then unlocks the door. It is standalone system controller which is used to generate random password whereas GSM Technology is used to send the password to authorized person's mobile phone via SMS. The RFID reader reads the id number from passive tag and send to the microcontroller, if the id number is valid then microcontroller send the SMS request to the authenticated person mobile number, for the original password to open the Locker, if the person sends the password to the microcontroller, which will verify the passwords entered by the key board and received from authenticated mobile phone. The user will be provided with an SMS application, to access the locker through GSM, by which it will indicate the locker to generate an OTP and send it to the user's mobile number through GSM module using SMS. If these two passwords are matched the locker will be opened otherwise it will be remain in locked position. This system will be more secure than other systems due to, two way password verification. This system also creates a log containing check-in and check-out of each user along with basic information of user.

KEYWORDS: : Microcontroller, GSM, SMS, RFID, OTP, Locker.

I. INTRODUCTION

The advanced locker security system will be providing a huge change in the locker systems, in which we will be using various components like the Arduino Uno, GSM Module, RFID, Micro-controller as well a concept called OTP, which is generally used in net banking for a safer wireless authentication. After looking at various proposed reference papers, with various concepts of locking systems being implemented, we came up with an advanced locker security system which can overcome various drawbacks provided by our traditional and biometric locker systems. It gives the user a stage to communicate with the embedded locker system, wireless and ubiquitously, for access.

By using the concept of OTP (One Time Password), we will provide a unique password to the user each time he or she accesses it. The user will have to authenticate via GSM and RFID. The proposed system will be implemented at a much cheaper cost compared to the biometric locker systems as the components used will be cheap, robust and fundamentally easy to implement. Hence, the proposed system can be implemented in banks, industries, offices, homes, etc. by overcoming the idea of simple lock and key mechanism. Looking at the overview provided by the advanced locker security system we get to know that it is a promising venture that will improve the quality of security.

II. RELATED WORK

In the two way random password generation idea[1], this paper describes that RFID technique is used to read user info and the GSM is used to receive and send SMS to authorized person's mobile. The description of the locker that will save the images of the intruder via cam and send a SMS to the authorized user using GSM Module[3]. The sending locker password to only register authorized compared to existing method/ methods[2].



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 5, May 2017

III. PROPOSED ALGORITHM

A. Design Considerations:

- Input voltage for GSM and LCD 5v.
- Input voltage for RFID, Locking mechanism (Servo motor) and the Keypad will be 3.3v. Arduino uno is micro-controller board based on the ATmega328P, acting as the central core of the complete system which is also beneficial to the system due to compactness, lower power consumption and a higher flexibility to high programming languages like C++.
- The MFRC 522 RFID is also used due to its compact size and extremely low power consumption capability.
- The system will be in a passive active state until, it senses the user's received message by the system.

B. Description of the Proposed Algorithm:

Aim of the proposed algorithm is to maximize security of the locker system by making it able to communicate to the user via SMS and generate OTP (One Time Password) each time the user accesses the locker. The proposed algorithm makes sure that the locker interacts with the authorized user only, using a three-way authentication for the user's identity.

The three-way authentication goes such as:

1. Authentication of user's mobile number:
The user sends an impromptu message to the locker via SMS, where the locker verifies whether the received mobile number from the message is the authorized user's mobile number [2]. After which if it is verified correctly and then an OTP is generated by the locker which sent to the authorized user's mobile number via SMS.
2. Authentication of the User's RFID Tag:
The user will be provided with a unique identification RFID tag, after the purchase of the locker, which will have to be flashed in front of the RFID reader for user's person identification, after receiving the OTP from the locker.
3. Authentication via OTP given to the user:
The user after correctly verifying his or her RFID tag, will input the received OTP into the locker via keypad and press '#' for ENTER. If the OTP matches correctly with the generated OTP by the locker, the user is given access to the locker.

Step 2: Random One Time Password Generating Algorithm:

Here, the concept of OTP (One Time Password) will be used, usually used in internet banking. This technique will be used to overcome [3]:

- 1) The singularity of the password.
- 2) Password being stolen by unauthorized user.
- 3) Limited input time period for the generated OTP.
- 4) Using alphanumeric values, the OTP will be generated.

This OTP will overcome brute force attack as after 3 tries the locker will lock-down for three hours and a notification will be sent to the authorized user.

IV. PSEUDO CODE

Step 1: Start

Step 2: The GSM module accepts the message sent to it by the user.

Step 3: The Arduino Uno verifies if it's the authorized user's mobile number.

If the mobile number is correct go to next step or else go to step

Step 4: The Advanced Locker System generates an OTP and sends it to the user's mobile number through SMS by the GSM Module.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

- Step 5: The Locker displays a message, using the LCD display screen, to the user to authenticate his/her RFID tag via RFID reader.
- Step 6: The user flashes his/her Tag in front of the reader.
If the tag is correctly verified by the Arduino then goto the next step else goto step
- Step 7: The locker displays message to enter the OTP, given to the user, into locker via keypad and press '#' to enter.
If the OTP correctly matches the generated OTP by the arduino then goto next step else goto step
- Step 8: Open the locker to the user to store or retrieve valuables.
- Step 9: Close the locker door, after using, and enter any key and press '#'. The door of the locker gets locked and the locker goes into an idle state waiting to detect a message sent by the user.
- Step 10: The Locker is reset and displays a message for the user to send the message again to get an OTP and start the authentication procedure all over again. After three wrong tries the locker will be locked down for 3 hours.
- Step 11: Stop.

V. SIMULATION RESULTS

The simulation study involves embedded locker system. The proposed system contains GSM, RFID, servo motor, LCD, alphanumeric keypad, and arduino uno. In which, the GSM module accepts and send the message to authenticate user, the arduino uno verifies that "is it authorized user's mobile number?", RFID is used for authentication purpose, servo motor is used as locking mechanism, LCD displays the message, OTP generator in the program used to generate OTP and send it to verified user via GSM module.

Thus by joining GSM, RFID, servo motor, LCD, alphanumeric keypad, and arduino uno (as the core micro-controller) we have implemented our proposed advanced locker security system. The image given below is the embedded system of our locker.

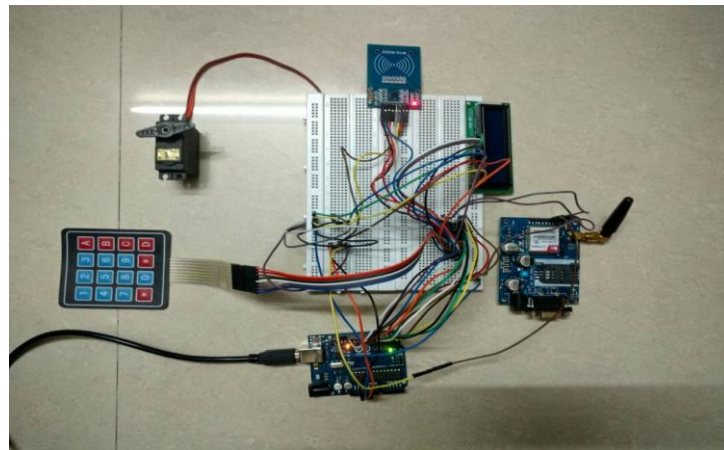


Fig.1. Advanced locker security system.

VI. CONCLUSION AND FUTURE WORK

The particular hardwares and softwares that are going to be used to construct this Advanced Locker Security System are clearly stated, given their functionalities, purpose and price we are sure to overcome the costliness of a biometric locker system and provide a better security system at much lower cost. Depending on our locker system's functionality we can say it can be used in homes, offices etc. It can also be used as a locking mechanism for the doors of our houses..

REFERENCES

1. R.Ramani, S. Selvaraju, P.Niranjan and S.Valarmathy, 'Bank Locker Security System based on RFID and GSM Technology', International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

2. Dr.(Mrs) Saylee Gharge, Honey Brijwani, Mohit Pugnani, Girish Sukhwani and Deepak Udherani, 'Two way password verification security system using RFID and GSM technology', International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 – 4847 Special Issue for International Technological Conference-2014.
3. Shweta S. Joshi, Vinayak Ekke, Pankaj Yedurkar and Ajit Lokhande, 'Locker Security System using GSM and Random Password', International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 04, April 2015.

BIOGRAPHY

Mrs. Milana Malvadkar working as an Assistant Professor in P.E.S Modern College of Engineering and is our guide for the project. **Radhika Hambire, Prutha Suroshi and Priteshsingh Chandel** are students pursuing Bachelor in Computer Engineering in the college P.E.S Modern College of Engineering, Shivajinagar, Pune. Our research interests are Computer Networks, Pervasive Computing and Embedded Operating Systems.