Chaotic Procure Key Generation and Digital Locking

[1]Veeravajhula. Sarvani, [2]Marripudagala. Sowmya, [3]Upthala. Sai Jyothi, [4]Bhimavarapu. Madhuri, [5]A. Narendra Babu
[1]Student, [2]Student, [3]Student, [4]Student, [5]Professor
[1] Department of Electronics and Communication,
Lakireddy Bali Reddy College of Engineering, Vijayawada, India

Abstract : At present there are many locking systems that are providing the highest security to the bank vaults involving the technologies like RFID, Biometric, OTP and cryptography yet, there are many hacking techniques developed to breach into the bank vaults. This hacking is possible only due to the usage of pseudo random numbers as the security keys. The replacement of these pseudo random security keys with true random security keys by using the chaotic system could be a greater advancement in the security systems. This paper presents the idea of generation of true random numbers in an efficient way and so can be used as the security keys for the digital locks which could be accessed only by the authorized personnel.

IndexTerms - **Cryptography, RFID, OTP, True random number.**

I. INTRODUCTION

Security is a defense against threats which provides an assurance of safety. Now and before security is one of the major concern in places like home, offices, institutions, banks, laboratories etc. in order to keep our data confidentially so that no other unauthorized person could have access on them. In olden days the security mechanisms are less in order to prevent unauthorized access. Nowadays lot of security mechanisms have been introduced for such places and applications. But along with a wide variety of security methods, the techniques of theft are also changing and it's increasing day by day.

Various security systems are available but, each system has its own pros and cons just to avoid one of the disadvantages of usage of pseudo random numbers that could be interpreted as the generation of the pseudo random number involves some logical codes rather a system that could generate the true random numbers sensing the real time variations in environment is proposed. The generation of true random number can be done using the chaotic generation algorithms[11] that are used as in the generation of keys in the cryptography which involve the large complex mathematical equations other than this another method is, to use the chaotic oscillators, which is an old technology avoiding these all cons the sensing of the real time variations in the light/dust particles in the surroundings can be in turn used to generate the true random numbers with a less complex and no code system.

This paper consists of several sections. Section II gives the literature survey about the existing systems. Section III describes the methodology of the developed system. Section IV presents the hardware implementation of the door lock. Section V presents the results of the developed system and section VII concludes everything mentioned.

II. LITERATURE SURVEY

This section describes the different technologies which are being used in secure door locking systems. Coming from past times, mechanical locks were used which are not much secure. Later with the advancement in technology, electronic locks have also been introduced. Going further password based electronic lock system in which generated password becomes crucial for access was introduced, RFID based access control electronic lock system explained in [1] which utilizes two main components i.e., the RFID tag and the RFID reader was developed. Here the value on the RFID tag becomes crucial for access. Later on biometric lock system which requires face recognition, finger print recognition, and voice recognition as explained in [4] and [3] came into existence. An encryption based door lock system was also developed [5] and [6] where the mechanism is that the original password will be masked by an encryption value which generates a new password for access.

One Time Password (OTP) is the latest step in security access systems [2].In this system the OTP generated will be unique and will remain for only short time and so becomes difficult to hack. Taking this advantage of One Time Password generation an even more efficient and highly secure system in which even the generated one time password is truly random is developed.

III. METHODOLOGY

The chaotic procure key generation is done by sensing the real time variations in the light intensities in the surroundings and digitalizing those variations to generate the pass key. Fig 1 shows the block representations of the chaotic procure key generator. The blocks involved in the chaotic procure generator are a sensing block, controlling block, communication block and the output block. These all blocks play a crucial role in the provision of security to the vaults.

Sensing block is used to generate the true random numbers depending on the variations in the sensed changing light intensities that are to be captured by the LDR (light dependent resistor). The most common type of LDR [9] has a resistance that falls with an increase in the light intensity falling upon the device (as shown in the image above). The resistance of an LDR may typically have the resistance rang of 5K Ω to 20M Ω.

The resistor in the RC tank circuit of the 555 timer operating in the astable multivibrator mode is replaced by the LDR. The astable multivibrator is used as the pulse generator with the varying pulse widths in accordance with the variations in the light dependent resistance values of the tank circuit which is responsible for the time period.

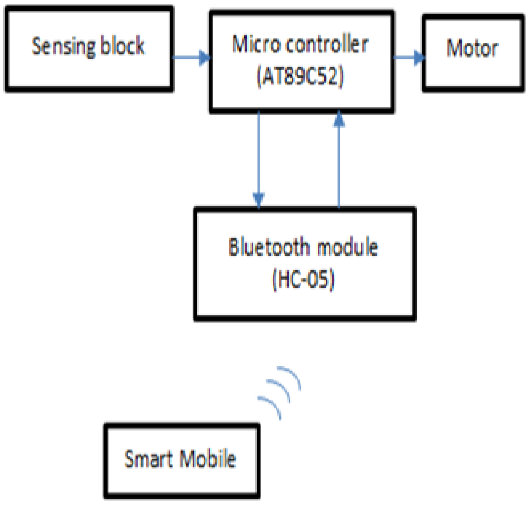


Fig 1 Methodology of locking system

The sensed data from the sensing block in further processed using the microcontroller and communicated to the authorized person through the Bluetooth module. If the code entered by the authorized personnel matches with the code that was generated and transmitted to the personnel smart mobile then the microcontroller activates the motor in turn unlocking the door. If the entered code does not match with the generated code then the microcontroller will activate the buzzer alerting the vicinity of the vault.

IV. HARDWARE IMPLEMENTATION

As shown in Fig 2 the heart of the controlling unit is the microcontroller AT89c52 [7] in this implementation. AT89c52 is an 8bit microcontroller belonging to Atmel’s 8051 family. This microcontroller is the one that is interfacing all the other hardware blocks like the sensing to the communication and output blocks

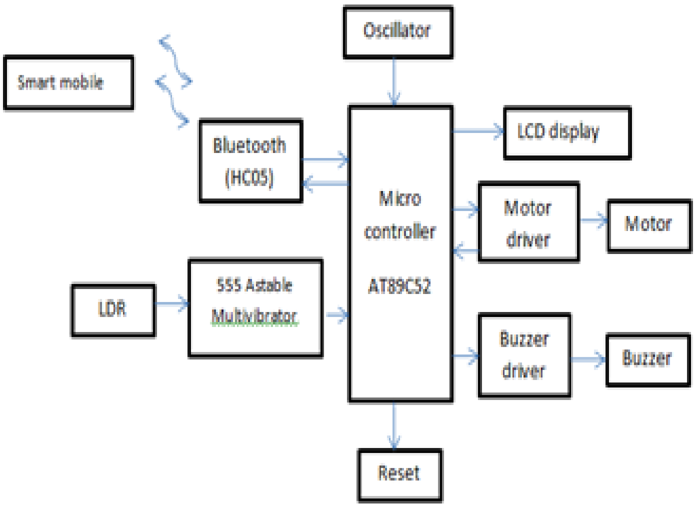


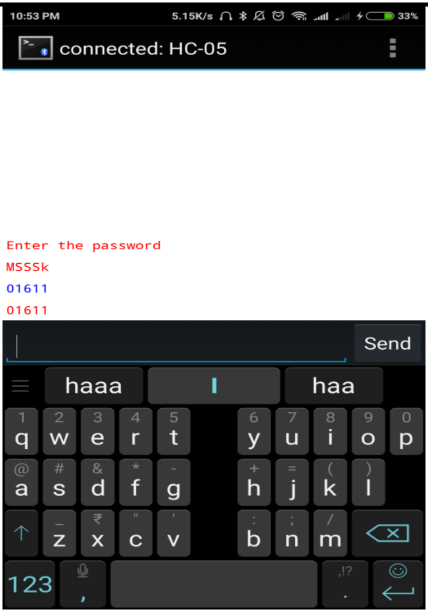
Fig 2 Detailed Architecture

The communication block will be a Bluetooth module which sends the initial request from the authorized personnel’s smart mobile to the controller which turns on the sensing block to generate the one time password. The generated five digit passcode will be later sent to the authorized personnel’s smart mobile through Bluetooth module. The initial request can only be sent by the authorised personnel as the activation of the whole system is protected with an additional password that is given by the individuals hence providing the maximum security to the whole system. Bluetooth module used in the system is HC 05 [8] a serial USART (universal synchronous asynchronous receive and transmit) system.

Output can be observed in two scenarios, if the motor rotated then the unlocking of the digital locks is happening else if the buzzer is activated then it means there is an unauthorised attempt to open the vault. The actuation on the two output blocks is performed by two drivers i.e., the motor driver and the buzzer driver. The motor driver used here is L293D [10] which is a dual H-bridge driver (IC).It has the capability of driving two DC motors simultaneously, both in forward and reversed direction. An active buzzer driver is preferred for driving the buzzer as it has the capability of producing sound by itself without needing an external frequency generator.

The smart mobile used contains an android application “Bluetooth terminal” which is a user interface through which the user should enter the required pass keys. Fig 3 shows the Bluetooth terminal display program where the system will be connected to the smart mobile through the Bluetooth protocol.

Once the smart mobile is connected then the password which activates the sensing block can be entered, so that the passkey can be generated and viewed to the authenticated personnel in a secure line on the Bluetooth display program shown in Fig 3.



10:53 PM 5.15K/s 33%

connected: HC-05

```
Enter the password
MSSSk
01611
01611
```

Fig 3 Blue Tooth Terminal

One Time Password also known as disposable passwords is a security mechanism where a unique password is generated each time that last only for few seconds. The utilization of this one time password mechanism is done using the Bluetooth terminal. The reception and submission of the generated passkey is done using the android application.

The chaotic procure key generator and digital lock contains an extra security measure which is not observed in any other digital locks i.e., the usage of a keypad attached with a touch sensor acting as a alerting system, whenever there is an unaware attempt (touch) to open the lock as there is no need of a keypad to enter the generated passkey.

V. APPLICATIONS

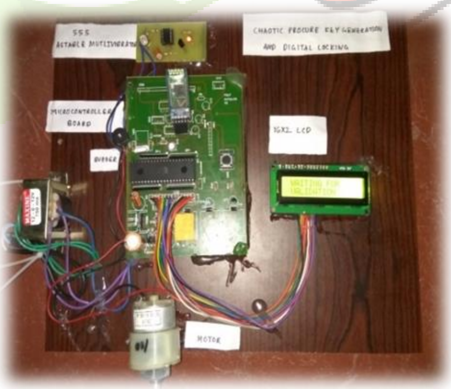
The generated true random number can be used as in different applications. Some of the areas where this can become helpful are given below

- In security critical areas like banks, houses and any business localities the true random number can be used as a pass key to secure the data, money and anything valuable
- In the field of cryptography, where the intended message is encrypted using a public or a private key and then decrypted at the receiver end for secured communication.

VI. RESULTS AND DISCUSSION

The chaotic procure key generation is done for the digital locks that to be used in any situation. This system is more secure though less complex in any situations.

Fig 4 shows the complete schematic of the chaotic procure key generator and the digital lock including all the blocks that are explained in the previous sections.



555 ASTABLE MULTIVIBRATOR
CHAOTIC PROCURE KEY GENERATION AND DIGITAL LOCKING
MICROCONTROLLER BOARD
16X2 LCD
BUZZER
MOTOR

Fig 4 Digital Locking System

The activation of the complete system is done when the power supply is given. The system waits for an event to be requested so that it can activate the sensing block to generate the one time password and the controller to assign the passkey to the vault. The event can be generated only after the assigned password is given correctly as shown in the Fig 5.

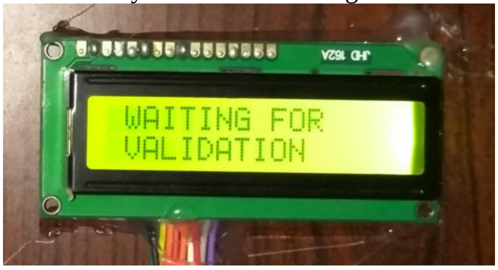


Fig 5 Waiting for event request

This system will oppose the unauthorised access to the vaults in two cases

- If the given password to start the system is not given correct.
- If the generated passkey doesn't match with the entered one.

Either of the above mentioned cases will activate the buzzer to alert the security if there is a breach by showing the message in the LCD screen as shown in the Fig 6.

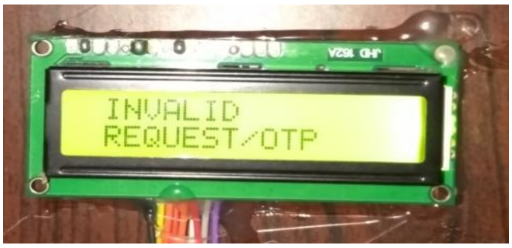


Fig 6 Alert message for unautherised attempt

In the case of correlated password and the OTP, the motor is driven in turn opening the door of the vaults. As shown in the Fig 7 the access to open the door message is appeared on the LCD display.

VII. CONCLUSION

The limitations of pseudo random number had replaced by the chaotic systems. Various studies have been reviewed regarding the electronic locking systems and in the area of cryptography algorithms. The chaotic procure key generator is developed for the application of digital locking. The system is designed to be cost effective, less complex and less power consumption. This chaotic procure key generation is done using limited hardware components utilizing the basic variations in the environment and the dust particles. Further advanced modules can be used as the communication interface. Hence the designed chaotic procure key generator is one of the advanced systems which cannot be hacked by anyone.

REFERENCES

[1] Meera Mathew, Divya R S"Super Secure Door Lock System For Critical Zones", IEEE 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum.
[2] Gyanendra K Verma and Pawan Tripathi, "A digital security system with door lock system using RFID technology," International Journal of Computer Application, Volume 5– No.11, pp. 6-8, August 2010.
[3]Arundhuti Chowdhury, "Revolution in authentication process by using biometrics," International Conference on Recent Trends in Information Systems, pp. 36-41, 2011.
[4]Madhusudhan M and Shankaraiah, "Implementation of automated door unlocking and security system," International Journal of Computer Applications, pp. 5-8, 2015.
[5]Jason Johnson and Christopher Dow, "Intelligent door lock system with encryption", US Patent Application Publication Johnson et al., pp. 1-92, June 2016.
[6] Rajan Jagdale, SankalpKoli, SaurabhKadam and SiddeshGurav, "Review on intelligent locker system based on cryptography, wireless & embedded technology," International Journal of Technical Research and Applications,pp. 75-77, March 2016.
[7] M. Mitescu I. Susnea,"Microcontrollers in Practice", The Springer Series in Advanced Microelectronics.
[8] Miss. Varda Kalidas Naik Ekoskar, Mrs. Anisha Cotta Miss. Naik Trupti Devidas,"Wireless communication using HC-05 Bluetooth module interfaced with aurdino," International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 4, April 2016.
[9] J.W. PUSTJENS,P.F. VAN OORSCHOT,"the resistor guide", First published 2012, All contents copyright © The Resistorguide 2013.
[10] L293x Quadruple Half-H Drivers, SLRS008D –SEPTEMBER 1986–REVISED JANUARY 2016 www.ti.com.
[11] M.I. Sobhy, A.-E.R. Shehata," Chaotic algorithms for data encryption," Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference.