GSM Based Smart Security Lock for Access Control Applications

Mitu Raj
Dept. of Electronics and Communication, Master of Technology in Embedded Systems, ERDCI-IT, CDAC, Trivandrum, Kerala, India

Abstract
Security of electronic devices is sometimes essential to defy any unauthorised access and to make them invulnerable to external interventions. Electronic Security Systems for Access Control are a class of security systems, which serve for the aforementioned purpose. In this paper, a GSM (Global System for Mobile Communication) Based Smart Security Lock is proposed to authorise access to electronic devices. The proposed system is a security lock, installed between the power supply and the device to be secured as a password controlled switch. The device can be locked with a programmable numeric password of any desirable length up to 15. The lock is also authorised to a unique phone number. The incorporated GSM module acts as a mean for enhancing security through a real-time two-way interaction between the system and the owner via SMS (Short Message Service). The Smart Security Lock comes with an inbuilt anti-tampering feature. Also a feature called freeze mode has been added for emergency security and sleep mode for saving power. The proposed system intends to put forth a reliable, low cost, potent and novel security solution for access control applications.

Keywords
Access Control Systems, Authentication, Electronic Security Systems, GSM, Home Security, Short Message Service

I. Introduction
An Electronic Security System refers to any electronic equipment that can perform security operations like surveillance, alarming, or controlling access to a particular facility or an area. Depending upon the area to be protected and possible threats associated with it, security systems may be classified into Access Control Systems, Surveillance Systems and Alarming Systems [1]. Access control systems' function in general is to control the access to a particular facility, area or an electronic device and to keep track of the access details. The quest for such systems started couple of decades before. Later on, an electronic lock system in which a coded data word stored in a key is compared against a master code to unlock or lock was invented and patented [2]. But it was not programmable by the user. In [3], a programmable electronic lock was introduced for use with lockers assigned for transitory or permanent use. It had a keypad for entering a sequence of digits. But the system was bulky, complex and was easy to infiltrate. Advancements in electronics over the last decade invented finest techniques for access control applications. RFID (Radio Frequency Identification) based and Biometrics based security systems have become two of the most popular Access Control Systems in recent times. Purely RFID based systems lack a solid security as the RFID tags may be used by anybody else to fake the authentication easily [4]. Biometrics based systems are highly expensive even though they provide an ironclad security. Hence a low cost, but a powerful security solution at the same time, is an attractive alternative to think about. The proposed system, GSM based Smart Security Lock belongs to such a category. It is a hardware lock to securely lock AC/DC driven electronic devices with a variable length numeric password. The system can be used to control the access to consumer appliances at home, computers and other hardware in the confidential sections of an office, industry, factory or private areas. It may also be implemented on electronic doors to control the entry to restricted areas, and on electronic lockers as an alternative to conventional lockers. It is stand alone and battery powered, and is installed between the power supply and the electronic device to be secured. Full specifications of the system are described in the next section. At the highest abstraction level, the proposed security lock is a password controlled switch as shown in the fig. 1.

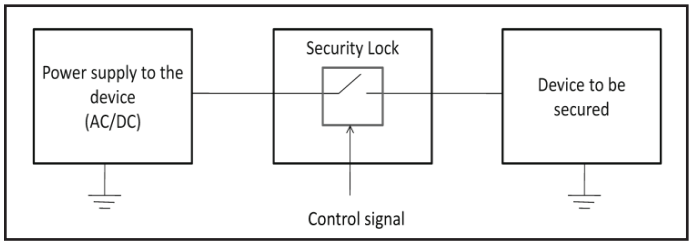

Fig. 1: An Abstract View of the Smart Security Lock

If the password entered by the user matches with the pre-programmed password, microcontroller asserts the control signal and the switch is closed, thereby powering on the device. Otherwise it remains powered off.

II. System Specifications
Following are the specifications of the proposed system presented in this paper.

1. The proposed system is a battery powered, microcontroller based security solution implemented as shown in Fig.1. It can be programmed to a desired numeric password of any length up to 15.
2. The Smart Security Lock is authorised to a unique phone number, which is assumed to be that of the owner.
3. Both password and phone numbers are updateable via SMS. Any trial access or wrong password attempts are alerted via SMS to the owner.
4. The Smart Security Lock comes with a freeze lock mode. After 3 wrong attempts on password, the lock is "frozen" indefinitely, until it is unfrozen by the owner via SMS.
5. The embedded GSM Module provides the mean for this two-way interaction between the owner and the lock. It enables the owner to send commands via SMS to freeze the lock, unfreeze the lock, change password, change the authorised phone number, and to retrieve the forgotten password.
6. The incorporated Anti-Tampering Module can detect any kind of tampering of the lock.
7. To save battery or reduce the power consumed by the system, a sleep mode operating feature has also been included.

III. Block Diagram Description

The following fig. 2. represents the block diagram of the proposed system.

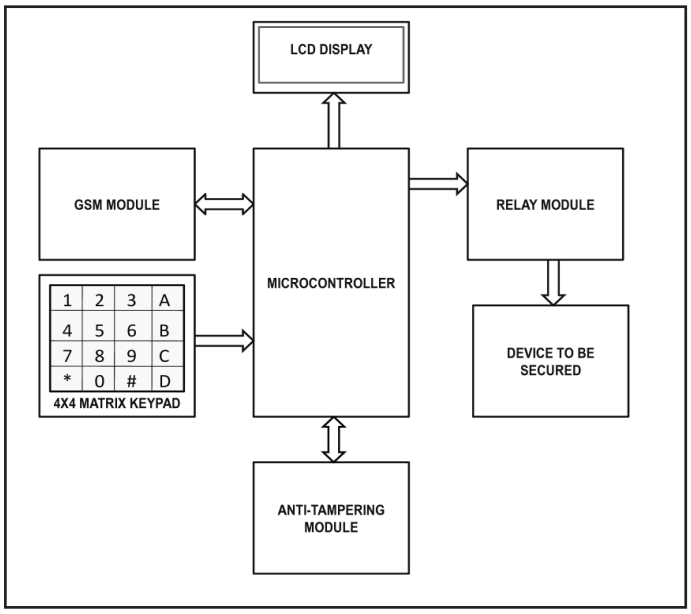

Fig. 2: Block Diagram of the Smart Security Lock

The Smart Security Lock consists of following modules: A Microcontroller, a 4x4 Matrix Keypad, a GSM Module, an Anti-Tampering Module, an LCD (Liquid Crystal Display) Module, a Relay Module and the Electronic Device to be secured by the lock. The functions of each block are described below in detail.

A. Microcontroller

The microcontroller controls the logic flow of the system. It contains the master program in the flash memory, and stores the password and the authorised phone number in the EEPROM (Electrically Erasable Programmable Read Only Memory).

B. 4X4 Matrix Keypad

4x4 Matrix keypad forms the primary interface between the user and the Smart Security Lock. It consists of 16 keys in rows and columns. The user inputs numeric password via this keypad. Besides 0 to 9, keys have been assigned in the keypad to lock/unlock, and clear input.

C. GSM Module

GSM Module constitutes the secondary interface of the Smart Security Lock. It permits a two-way communication between the owner and the Security Lock. The GSM Module is responsible for sending real-time SMS alerts to the owner, in the event of an unauthorised attempt to access the device. Another important job is to receive SMS commands from the owner and transmit it to the microcontroller serially.

D. LCD Module

LCD Module is the output interface of the lock. It displays the input, which the user is entering currently. The LCD also displays the current status of the lock; whether it is locked, unlocked, frozen, on sleep mode or busy. 16x2 display is used.

E. Relay Module

The Electronic Device to be secured is connected as external load of the Relay Module. The relay picks the control signal from the microcontroller, based on the password input by the user and does the ultimate switching of the device (ON or OFF). The end device may be electronic appliances like computers, fax, electronic door to restricted areas, electronic locker etc.

F. Anti-Tampering Module

It consists of an accelerometer and a buzzer alarm. The function of the Anti-Tampering Module is to detect whether the Smart Security Lock is being physically intruded or tampered i.e; whether somebody is trying to unscrew, move, alter or destroy the lock. Low power dynamic accelerometers with high precision have been designed for microcontrollers. It can measure dynamic acceleration due to tilts, motion, shocks and vibrations in 3 axes and hence may be employed here to detect tampering easily.

IV. Flow of Logic

As shown in fig. 1, the Smart Security Lock is a password controlled switch which closes only when the input password matches with the stored password. The initial requirement is that, an embedded program has to be written, compiled and executed in the microcontroller to burn the desired password and phone number into its EEPROM as stream of bytes. This will be the credentials used for the authentication purpose. The top level algorithm of the basic functionality of the system has been represented as a flowchart in the fig. 3. The main program, which has to be coded later into the microcontroller, implements this logic.

A. Operation of the System

The Smart Security Lock has 5 modes of operation; Locked mode, Unlocked mode, Freeze mode, Busy mode and Sleep mode. In Locked mode, the electronic device is powered off or said to be locked. In Unlocked mode, the device is powered on from the supply or said to be unlocked. In Freeze mode, it's not possible to access the keypad anymore. The device is then said to be frozen. It can now be unfrozen only by an SMS by the owner. Freeze mode thus prevents malicious attacks on the lock. If the system is currently furnishing an SMS request, the system is said to be in Busy mode. No keypad input is accepted until it comes off the busy mode. Sleep mode is activated when nobody is using the keypad and if it is in an idle state for a few minutes. During the sleep mode the LCD display backlight is switched off, thus saving the battery. The user first inputs a numeric password via keypad and press the lock/unlock key.

When the lock/unlock key is pressed, the microcontroller compares the input password with the stored password in its EEPROM. If both match, the device is either locked or unlocked depending on its current state. If both don't match, it is counted as an unauthorized access or wrong attempt and the device remains in its previous state. In both cases proper SMS alerts are sent to the owner. Thus a secured translation from locked to unlocked state and vice versa is ensured. If the number of wrong attempts become 3, the device is frozen. Incoming SMS can interrupt the normal operation of the system by putting it in busy mode. When in busy mode, the source phone number of the received SMS is deduced first and authenticated against the stored phone number. If the authentication is successful, the SMS content is decrypted and the requested action is executed. If the authentication fails, the SMS is ignored and comes out of the busy mode.

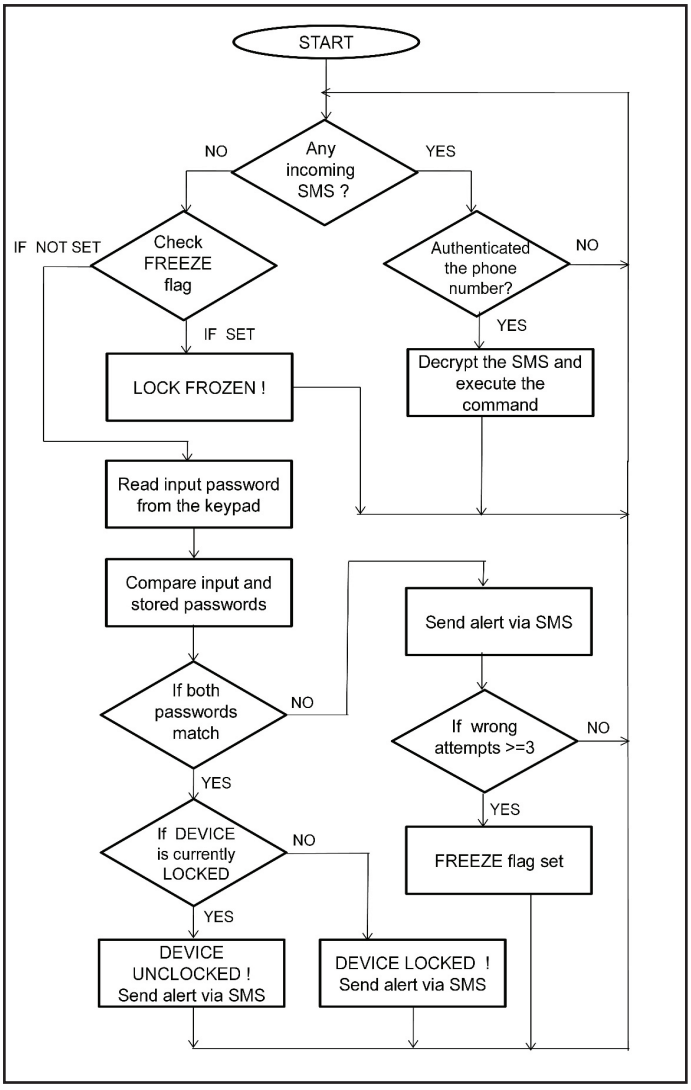

Fig. 3: Top Level Flowchart of the System

B. Operation of the Anti-Tampering Module

The embedded Anti-Tampering Module consists of a dynamic accelerometer and a buzzer alarm. Its algorithm is represented as a flowchart in fig. 4 below.

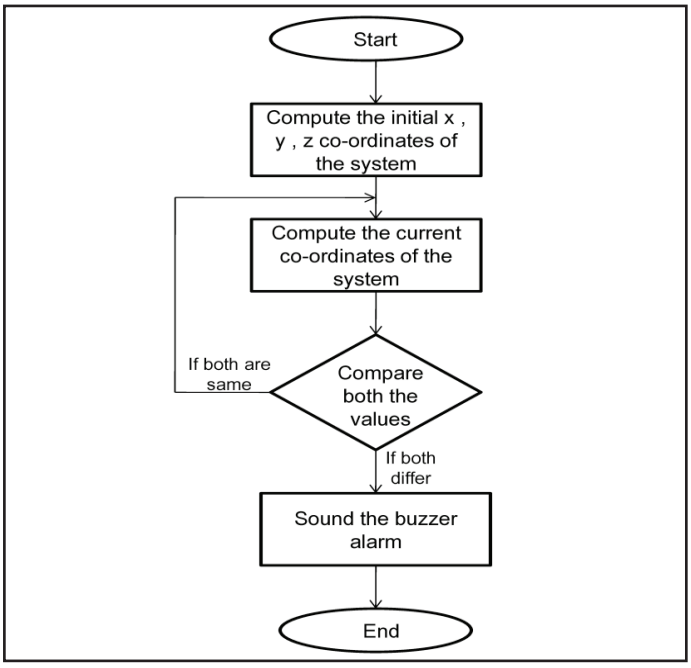

Fig. 4: Flowchart of the Anti-Tampering Module

The function of the module is to detect tampering, any kind of physical intrusion or mishaps in the smart security lock. Accelerometer can find the coordinates of the position of the lock in 3 axes and pass this information to the microcontroller as voltage levels. On reset or at the start, the initial coordinates of the position of the Smart Security Lock are calculated and stored. The current system coordinates are then continuously monitored by the microcontroller, and are compared against the initial values. Any kind of tampering of the Security Lock like unscrewing the body of the lock, trying to misplace or remove the lock, can cause shocks, vibrations or movements in the position of the lock. It will result in a change in the current system coordinates. This change is detected and the buzzer alarm beeps. An SMS alert is also sent to inform the owner.

C. SMS Requests and their Decryption

Following are the SMS requests from the owner's phone, which are furnished by the GSM Module of the lock.

- FREEZE – To freeze the lock in case of emergency or suspicious access.
- UNFREEZE – To unlock from the freeze mode.
- UPDATE<SPACE><NEWPHONE NUM> - To update the phone number authenticated with the lock.
- CHANGE<SPACE><OLD PASSWORD><SPACE><NEW PASSWORD> - To change the password of the lock.
- FORGOT – To retrieve the password, if forgotten.

Decryption of incoming SMS is necessary to identify the sender and the message content. This job is done by the microcontroller. Whenever an SMS is received, the GSM Module transmits the corresponding information serially to the microcontroller in ASCII (American Standard Code for Information Interchange) format. The information contains the source phone number, timestamp, and the message content. This information always has a definite and deducible structure and hence the source and the content of the message can be easily decrypted and analysed using a simple array comparison algorithm. It ensures that only valid SMS from the authorised phone number can manipulate the security lock.

D. Security of SMS and Comparison with Other Security Locks

SMS systems are inherently confidential between sender and receiver by means of cryptographic algorithms like A5 [5]. The research in [6] reviews the SMS security by outlining the different security issues related to SMS systems and the mechanisms and techniques used to overcome these issues during the entire SMS transmission circle from the mobile source to the final mobile destination. It mentions techniques like end to end encryption, which may be implemented in Smart Security Lock to further enhance security.

Biometric based security locks are highly secured and popular these days. But they are very expensive choices to be considered on low cost platforms [7]. Fingerprint sensor itself costs around 50 US dollars in market. RFID based security locks are cheaper and easier to implement. But the reliability of such locks is questionable because the tags may be easily procured and used by anybody else to fake authentication. Other existing programmable security locks, just use fixed length key codes to lock/unlock. The proposed Smart Security Lock makes use of variable length numeric password. The password can be of any length up to 15; Hence, the possible no. of combinations is very high, $N = (10^{15} + 10^{14} + 10^{13} + \ldots. 10)$. Thus it makes the password key difficult

to break. Also, the incorporated GSM Module provides a secured bi-directional communication using SMS, which strengthens the security [8]. In addition, the Anti-Tampering Module ensures that the lock is not physically intruded. With the aforementioned components, the whole system can be implemented on PCB (Printed Circuit Board) under 30 US dollars (unit cost), which is cheaper compared to Bio-metrics based security locks. Thus the proposed Smart Security Lock puts forth a strong security solution for low cost applications, especially in home security and office security.

V. Conclusion

Access control is an essential aspect in the security of electronic devices. In this paper, a novel security solution is proposed, to build password secured access control systems at low cost. On the upside, the proposed GSM based Smart Security Lock promises a reliable, portable, low cost security solution with an emergency freeze mode and low power sleep mode features, and also proven security against tampering. It also offers many windows for modifications in the future. The proposed version of the smart lock is authorised only to a single phone number. It can be extended to support multiple phone numbers. Appending bio-metrics increases the security, but with the overhead of increased expense.

References

[1] Robert Pearson,"Electronic Security Systems", First ed. Butterworth-Heinemann, USA, 2006.
[2] Fowler John, Perron Robert,"Digital Lock System Having Electronic Key Card", U.S Patent 3 859 634, January 7, 1975.
[3] Yucel. Keskin, K.; Asil Gokcebay, T.,"Programmable Digital Electronic Lock", U.S Patent 5 894 277, April 13, 1999.
[4] Yan Zhang, Paris Kitsos,"Security in RFID and Sensor Networks". 3rd ed. CRC Press, USA, 2016.
[5] Chouhan, A.; Singh, S.,"Real-Time Secure End to End Communication over GSM Network", International Conference on Energy Systems and Applications, November 2015, Pune, pp. 663-669.
[6] Medani, A. et al.,"Review of Mobile Short Message Service Security Issues and Techniques Towards the Solution", Scientific Research and Essays, No. 6, pp. 1147-1165, November 2011.
[7] Smith, D. et al.,"Face Recognition on Consumer Devices: Reflections on Replay Attacks", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 4, pp. 736-745, April 2015.
[8] Hari Prakash, B. et al.,"A Review on Security in Mobile Communication Technology", International Journal of Engineering Science and Computing, No. 6, pp. 4618-4620, May 2016.

Mr. Mitu Raj received his B.Tech degree in Electronics and Communications from Cochin University of Science And Technology in 2013. He is currently pursuing M.Tech degree in VLSI and Embedded Systems at Electronics Research and Development Center of India - Institute of Technology. From 2013 to 2014, he worked as System Engineer at Infosys Ltd, Pune, India. His fields of interest include embedded systems design, embedded software development, embedded systems testing and IP (Intellectual Property) core design.