This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2017.2756876, IEEE Sensors Journal

Multi-Level Security Embedded with Surveillance System

Sanket Goyal, *Student, SRM University*, Pranali Desai, *Student, SRM University* and Vasanth Swaminathan, *Assistant Professor, SRM University*

***Abstract*—Graveness of Guarding is an essential component of any system or organization in an increasingly hacking environment. Layers of protection are necessary. This paper presents a model to develop a multilevel security system. To reach or access inner most circle, three stages of security system endorsement will be necessary, making it the primary level of security. These include the Hex Keypad, Bluetooth & RFID. The valuables in the inner vault are further secured with a secondary system completely separate from the primary, consisting of a Fingerprint Scanner. Any security breach detected will alert the authorities with the help of a GSM Shield, therefore taking the necessary response immediately. Continuous surveillance with online streaming is also demonstrated using Raspberry Pi and a Digital Camera, further safeguarding the valuables.**

***Index Terms*— Bluetooth module, GSM Shield, Hex Keypad, Raspberry Pi, Raspi Camera, RFID**

I. Introduction

Automated security system has been much in demand since a decade now, whether it is for an automated home [12] or an office with security [1]. This model puts forward a method to secure a high level organization with a multi-level security system. The three levels consists of a hex keypad locking [2], [13], Bluetooth code [3], [11] and RFID tag [4]. All three have to be passed to reach the innermost circle. The innermost circle is where the important items have been placed. The secondary unit consists of a security system based on Raspberry Pi [5], [15].

Raspberry pi camera has been used in this system but unlike [6] this paper not only helps to capture images but also helps for a 24*7 surveillance of the innermost circle on the host IP address. The important part being the surveillance does not start only when some motion is detected [7], in fact it is continuously streaming. If in the innermost circle any item has to be accessed, the pressure sensor has to be deactivated by the fingerprint module [8], so only a top-level authorised person can touch the item. In case the pressure sensor is not deactivated GSM module [14] sends a message to the all the authorised mobile [9]. Risk analysis of the system has not been taken place which can add to one of the most important innovation [10].

II. Overview of Home Automation

A. Block Diagram

The entry into the premises is controlled with the help of two different security protocols. The first protocol has an Arduino microcontroller as its control unit, which has as its input components, the Hex Keypad, Bluetooth module and RFID. These three modules have their predefined coded setting which has been fed into the controller. The output from the controller are three actuators attached with each of the sensor modules to open the respective door, when the correct key is entered. A push button is attached on the inner side of the wall which is used to close the door, just opened, after entering into the premises. Fig. 1 shows the components used in the system.

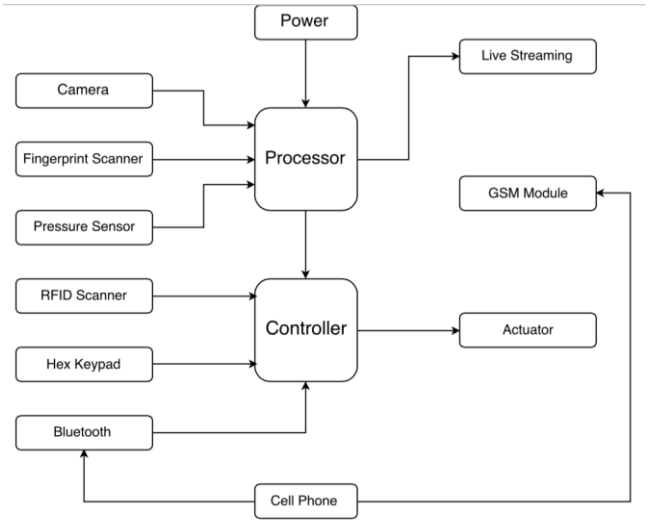

Fig. 1. Block Diagram

The second protocol consists of a Raspberry Pi microprocessor as its control unit. The input components here are Fingerprint Sensors and the pressure sensor. The output of the readings obtained from the input units can be recorded with the help of a GSM module. A Raspi cam is connected to the processor for continuous live feed on the servers.

Manuscript received August 3, 2017; revised September 20, 2017; accepted September 20, 2017. The associate editor coordinating the review of this paper and approving it for publication was Prof. Kazuaki Sawada. (Corresponding author: Sanket Goyal.)

S. Goyal is with the Department of Mechanical Engineering, SRM University, Chennai 603203, India (e-mail:sanket193@gmail.com).

P. Desai and S. Vasanth are with the Department of Mechatronics Engineering, SRM University, Chennai 603203, India.

Digital Object Identifier 10.1109/JSEN.2017.2756876

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2017.2756876, IEEE Sensors Journal

B. Work Flow of the Project

To reach to the innermost circle or the secondary security circle of the model, multiple loops of security have to be passed. The first one consists of digital locking system using Hex keypad, once the correct passkey has been entered the door opens and you are now in the second loop where you need to send a particular code to the Bluetooth module which will open the next door. The third loop consist of RFID scanner which will require authorised tag to open the door. This has been shown in Fig. 2. Once a correct tag has been used you are now in the secondary security circle.

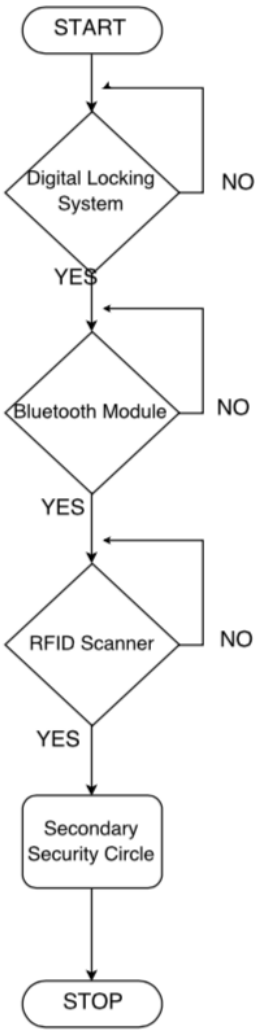

Fig. 2. Flow Chart for Primary Circuit

This has the most valuable items placed on it. Powered with a completely different unit, this vault is completely isolated from the exterior system. Placed under the valuable items are pressure sensor which are activated once an item is picked from the vault. If the fingerprint sensor scans the correct fingerprint, then there is no alert message of danger are sent via the GSM module. If the goods are picked, without the protocol, the GSM module, alerts the authorities.

Apart from this there is a continuous live feed, from the raspberry pi camera to the servers for better safety and 24*7 video feed of the vault. Fig. 3 represents the inner security loop with the flow of the events occurring. If the prints are matched, the goods can be accessed without any difficulties.

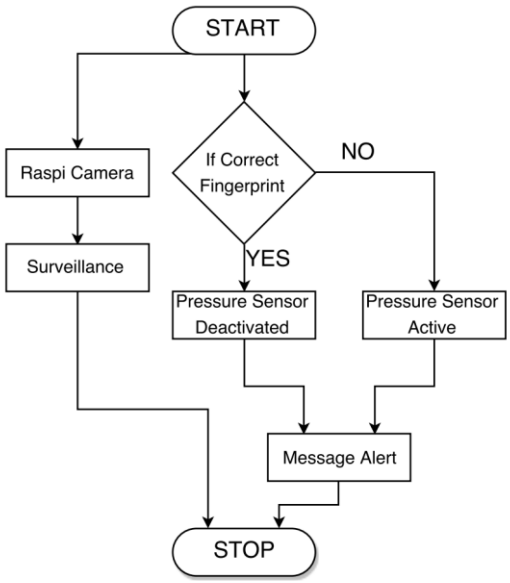

Fig. 3. Flow chart for Secondary Circuit

C. Circuit Diagram for the project

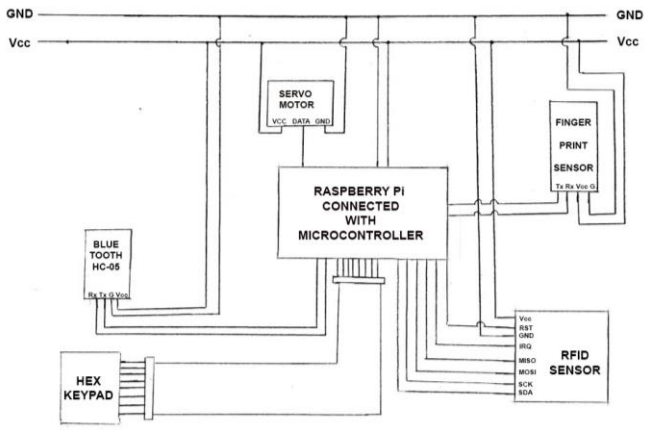

Fig. 4. Circuit Diagram

The connections for all the sensors has been shown in Fig. 4. The wiring for the prototype model has been accomplished keeping in mind the above circuitry. Each sensor is connected with the processor and is given Vcc and GND supply. Different number of input ports are required for different sensors. Hex Keypad used has eight input ports whereas the fingerprint module used has two.

III. Design and Implementation

A. Hex Keypad

In this multi-level security, Hex Keypad is the primary authentication to walk into the premises. A 4*4 membrane based Hex Keypad, as in Fig. 5, when given the correct

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2017.2756876, IEEE Sensors Journal

password, rotates the servo motor for opening the door. The passkey when entered, sends a signal to the Arduino, which processes it, based on the keys pressed. If the sequence of the pressed keys is according to the predefined code, a signal is sent to the actuator to unlock the door. If the sequence of pressing the keys changes from the already set pattern, the door remains locked. The specifications are in Table 1.

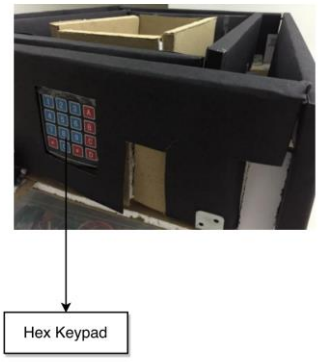

Fig. 5. Hex Keypad

Table I
Hex Keypad

Parameter	Specification
Maximum Rating	24 Volt DC, 30mA
Operating temperature	32 °F to 122 °F

B. Bluetooth

The secondary stage of safety is governed by wireless mechanism, based on Bluetooth signals. A Bluetooth module HC 05 is placed near the door. When a person want to go into the premises, the person, types in the authorized code into a mobile phone application which, if correct, actuates the motor via the microcontroller or keeps the door closed. Considering the fact that the authorized code is known to the authorized personnel only, it is a guaranteed approach for maximum security.

C. RFID

The tertiary level of security consists of a RC522 RFID tag system. Each tag has its unique identity number which has already been pre-coded into the system. As soon as a registered RFID tag is brought near the receiver (Fig. 6), the code for this particular tag is matched with the pre-registered code stored and the signals are sent to the actuator to perform its work. If the tag is not from an authorized personnel, the codes do not match and the actuator does not receive any signal. As it is known that each RFID tag has its unique identity, hence every time a tag is used to enter into the safe, the key can be tallied with the person who is authorized with that particular tag from the logs in the system.

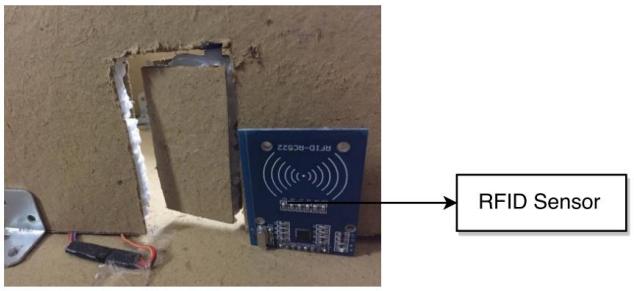

Fig. 6. Radio Frequency Identification

D. Pressure Sensor

An array of pressure sensors have been attached just under the valuables. As soon as there is a change of pressure sensed when the object is removed from its original place, a signal is sent to the processor, which in turn alerts the authorities. The pressure sensors are deactivated once the authorized fingerprint is scanned on the scanner, allowing the goods to be accessed with ease.

E. Fingerprint Sensor

After passing through all the three checkpoints, the final security present in the system is a fingerprint scanner R305. The key point of this scanner is, that it has been attached to a secondary processor unit and it is given a separate supply. To access the valuable item, allowed only to the top officials their fingerprint has to be scanned. As soon as the prints are matched, the pressure sensor present under the valuable objects are deactivated, allowing the good to be accessed. The key point of attaching this system is not to get inside the premises but for accessing the good by the authorized personnel only. A scanner is shown in Fig. 7 with its specifications for operation in Table 2.

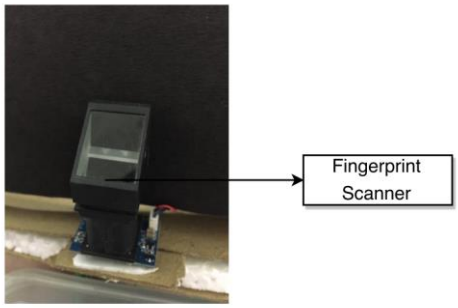

Fig. 7. Fingerprint Scanner

Table II
Fingerprint Scanner

Parameter	Specification
Supply Voltage	3.6 - 6.0VDC,
Operating Current	120mA max
Interface	TTL Serial

F. GSM Module

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2017.2756876, IEEE Sensors Journal

A GSM SIM900 module has been connected to the secondary security unit of the premises. The module is paired up with the microprocessor Raspberry Pi. Any working sim card can be put into the module, making it user friendly. The functioning of this module is such that, whenever the goods from the inner room are accessed without the correct protocol, this module sends out alert messages to the authorities for the required action to be taken. If the correct protocols are followed, there is a message alert is sent, so that the information of the accessed good can be recorded properly.

G. Raspberry Pi Camera

This Raspi Camera has been used in this model which is used for the online streaming. Connected with a Raspberry Pi, it is shown in Fig. 8.

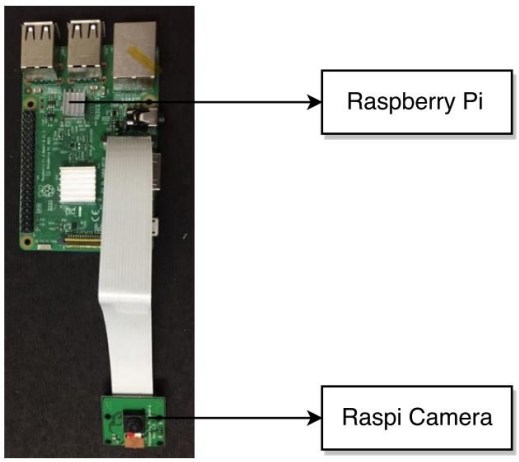

Fig. 8. Raspi Camera

Online Streaming of the innermost circle is done using Raspberry pi processor which can be viewed by typing the IP address of the host in any web server. Thus the activities taking place in the innermost circle can be viewed anytime and anywhere when you have an internet connection, thus ensuring the security. Table 3 gives the specifications for the same.

Table III
Raspi Camera Specifications

Parameter	Specification
Pixel Size	1.4 µm × 1.4 µm
Focal Length	3.60 mm +/- 0.01

H. Software

Arduino IDE has been used to program the Arduino and Arduino modules. Raspbian Operating system has been loaded on the SD card with NOOBS OS which is necessary to boot the Raspberry pi.
The coding of the sensors and modules attached to the raspberry pi has been done on the python platform. Coding on python can be done either by using the shell or by python software IDLE.

IV. CONCLUSION

Achieving the multi-level of security has been observed in this model, which consists of two different mechanisms to reach the vault and to access the good in the vault, powered by different powering units. The primary system consists of three things, namely the Hex Keypad, Bluetooth module and the RFID. All of the three systems have a coded password, which is known to the authorized person who has the clearance to enter into the next level only. Fig. 9 shows us the model for Primary Level of Security, working on the first protocol.

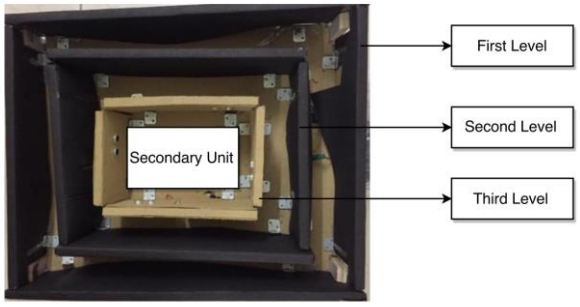

Fig. 9. Model for Primary Level of Security

The secondary security system, works on a second protocol i.e. it is in terms with accessing the goods stored inside the vault.

Table IV
Comparison of Sensors

	RFID	Bluetooth	GSM	Fingerprint	Hex Keypad
Model	RC522	HC 05	SIM 900A	R305	4*4 Matrix Keypad
Range	4 cm	10 m	Cellular Range of SIM	Direct Contact	Direct Contact
Operating Voltage (DC)	3.3 V	3.3 - 5 V	3.2 - 4.8 V	3.6 - 6 V	4 - 5 V
Application	Security	Data Transfer	Text Notification	Security	Alphanumeric Input
User Interface	RFID Tag	Smartphone	SMS	Fingerprint Scan	Membrane switch

The comparison for all the sensors used has been tabulated in Table IV. Depending upon the application and the user interface, it is observed that each and every sensor has a specific usage in the project. The operating voltage for all the sensors is within 5 volts, which is the output we obtain from our controller.

I. Future Scope

In the future aspect of this model, we look forward to implement image processing using the Raspi Camera to detect who entered inside the inner circle. This will help us have logs of all the people entering inside the vault. Laser modules can be used which are kept high when any of the level is not deactivated and if in that vicinity an intrusion is detected, lockdown of the system can take place, locking the intruder inside.

It is seen that the model built can be easily scaled up for real time applications, with regard to the security of the premises. The model explains 4 different mechanisms for having the premises safe, out of which any combination of sensors can be attached for the safety. It is not necessary to attach all four of them, together.

V. REFERENCES

[1]. Deepali Javali, Mohd. Mohsin, Shreerang Nandanwar and Mayur Shingate, Home Automation and Security System Using Android ADK, IJECCT, Volume 3 Issue 2, March 2013.

[2]. Vinoth Kumar Sadagopan, Upendran Rajendran, Albert Joe Francis, Anti-Theft Control System Design Using Embedded System, IEEE, 2011, 978-1-4577-0577-9/11.

[3]. Rajeev Piyare,Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone , IJIOT, 2013, 2(1): 5-11.

[4]. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of things: Vision, applications and research challenges,Ad Hoc Networks 10 (2012) 1497–1516.

[5]. P.Vigneshwari, V. Indhu, R.R. Narmatha, A.Sathinisha, J.M.Subashini, Automated Security System Using Surveillance, International Journal of Current Enginnering and Technology, Volume 5, No.2, April 2015

[6]. K.Gopalakrishnan, V.Sathish Kumar, G.Senthilkumar Embedded Image Capturing system using Raspberry pi system, IJETTCS, Volume 3 Issue 2, March - April 2014.

[7]. Sanjana Prasad, P.Mahalakshmi, A.John Clement Sunder, R.Swathi,Smart Surveillance Monitoring System Using Raspberry PI and PIR Sensor ,International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7107-7109 .

[8]. Dhvani Shah, Vinayak Bharadi,IoT based Biometrics Implementation on Raspberry Pi,Procedia Computer Science 79 (2016) 328 – 336.

[9]. Prakash Kumar and Pradeep Kumar, Arduino Based Wireless Intrusion Detection Using IR Sensor and GSM, IJCSMC, Vol. 2, Issue. 5, May 2013, pg.417 – 424.

[10]. Andreas Jacobsson, Martin Boldt and Bengt Carlsson, A Rish Analysis of a Smart Home Automation System, Future Generation Computer Systems 56, 2016, pg.719-733.

[11]. Nupur K. Sonawane,Payal D.Wwaghchavre, and Kajal A. Patel, Bluetooth Based Device Automation System Using Cellphone ,IJCAIT, Vol. 7, Issue I Oct.-November 2014, pp 136-141.

[12]. Shiu Kumar, Ubiquitous smart home system using android application, IJCNC, Volume 6 No.1, January 2014.

[13]. Azani Cempaka Sari, Anita Rahayu, and Widodo Budiharto, Developing Information System of Attendance and Facebook Status for Binus University's Lecturer Using Raspberry Pi Architecture, ICCSCI 2015.

[14]. Mahesh N. Jivani, Gsm based home automation system using app-inventor for android mobile phone, IJAREEIE, Vol. 3, Issue 9, September 2014, pp 12121-12128

[15]. Vladimir Vujovic´, Mirjana Maksimovic´, Raspberry Pi as a Sensor Web node for home automation, Computers and Electrical Engineering 44, 2015.

VI. BIBLIOGRAPHY

Sanket Goyal was born in Bijnor, India. He completed his higher school from Manav Rachna International School in the city of Gurgaon and his BTech is in Mechanical Engineering (batch – 2018) from SRM University, Chennai

Starting young in fields involving STEM, he has participated and won various awards in the competitions organized by FIRST. He now has broadened his spectrum and focuses more on research areas involving IOT and Automation. Wanting to spread the knowledge gained, he created a YouTube Channel named Robomechtrix. This team of five uploads different videos on theoretical and practical concepts in a systematic manner regularly.

Mr. Goyal was a recipient of the Gold Medal for the best paper award on the occasion of research day in the year 2017 at his University.

Pranali Desai was born in Baroda, Gujarat. She grew up there and also completed her schooling from the Bright Day School in Baroda. Her BTech is in Mechatronics Engineering (batch – 2018) from SRM University, Chennai

Her base is in Mechatronics Engineering, and her areas of research focus mainly on automation, security, and IOT.
Always inclined towards mathematics, she wants to pursue Robotics Engineering as her graduate study. She also manages a YouTube Channel named Robomechtrix along with four other students. The channel helps student around the world both in academics or practical projects.

Miss. Desai has also authored a paper on "Home Automation Embedded with Security." The same paper won the Gold Medal for the best paper on the Research day of SRM University in 2017.

S.Vasanth received the B.E. degree in Electronics and communication Engineering from Anjalai ammal mahalingam engineering college, Thanjavur, in 2010 and M.E degree in Mechatronics from Madras Institute of Technology, Anna University, Chennai in 2012 and is currently pursuing Ph.D. degree in SRM University. Since 2012, he has been an assistant professor with the Department of Mechatronics Engineering, SRM University, Chennai. His research interests include intelligent service robots, vision-based robotics and visual servoing.