ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (28-34), Month: April - June 2018, Available at: www.researchpublish.com

Security in Multi Level Embedded System for Surveillance

[1]Nisha V M, [2]Prof Sheela S V

PG student, Department of InformationScienceandEngineering, BMSCE

***Abstract*: the paper explains the structure and development in the field of multilevel security system. Consequences in control and protection are one of the most essential components of any system or organization in an increasingly hacking environment. Protection in layers is also necessary. To access or reach the inner most circles, there are mainly three stages of security system required, in order to make primary level of security. It can be Hex Keypad, Bluetooth, and RFID. The secondary system is completely separate from the primary system, which mainly uses scanning of fingerprint. Any act of breaking the security system will be detected and will alert the authorities with the help of a GSM Shield, and takes the necessary response immediately. Online streamingis used along with continuous surveillance is also demonstrated using Raspberry Pi and a digital camera, further safeguarding the valuables. In the above context, understanding the misuse of the potential misuse of the information that are related to risks such as homes and end-users and also forming methods for security enhancement of measures in the design that are not straightforward and requires a substantial investigation.**

***Keywords:* Bluetooth module, GSM shield, hex keypad, Raspberry Pi, raspy camera, RFID.**

I. INTRODUCTION

Over a few decades automated security system is in much more demand, either it is for home [12] or a security for an office [1]. This structure forwards a method in multilevel security system for a secured level or organization. The three levels mainly consist of a hex keypad locking [2,13], Bluetooth code [3,11] and RFID tag [4]. To reach the inner most circle all three levels has to be passed. The important items have been placed in the innermost circle. The next level secondary unit consists of a security system that is based on Raspberry Pi [5,15].This system uses a raspberry pi camera to capture images and also helps surveillance of the innermost circle on the host of IP address for 24*7 [6] . One of the most important part the surveillance is that is does not start only when some motion is detected [7], instead it idea continuous streaming. Considering a condition if any of the item has to be accessed from the innermost circle the pressure sensor has to be deactivated by the fingerprint module [8], so that only an authorized person can touch the item. In a situation where pressure sensor is not deactivated, GSM module [14] will sends a message to the all the authorized mobile [9]. Risk analysis of the system has not been taken place because it can add to one of the most important innovation [10].Home automation may include centralized control of lighting and other systems, to provide improved comfort, energy efficiency and security. Infrastructure such as trusted operating system are an important components of a system, but in order to fulfill the criteria required the system must provide a user interface that is capable of allowing a user to access and process content at multiple classification levels from one system. The device which has low cost and scalable to less modification is much more important. It represents the structure and implementation of automation system that can monitor and control home appliances through android phone or tablet**.**

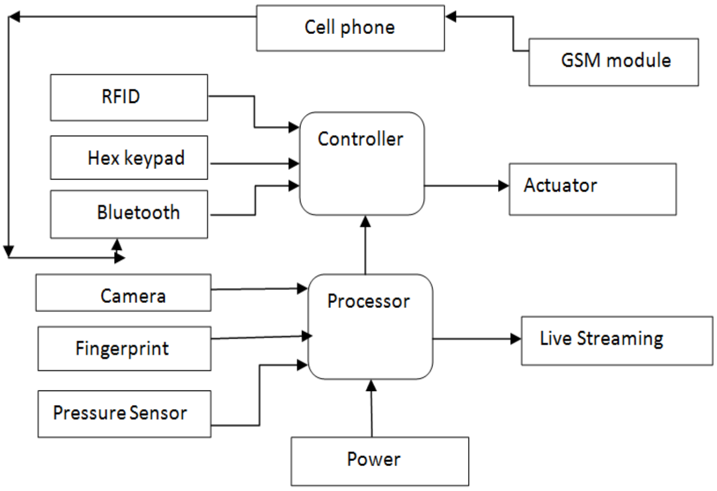


Fig. 1

II. OVERVIEW OF HOME AUTOMATION

A. System Architecture:

There is mainly two type's security protocol for the entry into the premises. The first security protocol is a Adriano microcontroller which has control unit that includes components such as the Hex Keypad, Bluetooth module and RFID. All the above three modules has a pre defined code setting which has been added in the controller. The output from the controller has three actuators that are attached with each of the sensor modules opens only when the correct key is entered by the user. At the inner wall of the door a push button is attached to close the door when just opened after entering the premises. The second protocol has of a Raspberry Pi microprocessor as its control unit.

B. Work Flow of Secondary Circuit:

Multiple loops of security have to be passed in order to reach to the innermost circle and the secondary security of circle. The first is the Hex keypad using digital locking system; once the correct passkey is entered the door opens.

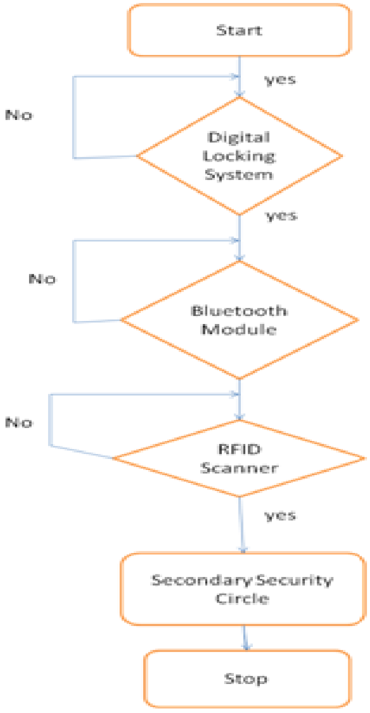


Fig. 2: Flow chart for primary circuit

The second loop where particular code will be sent to the Bluetooth module which will open the next door. The third loop is the RFID scanner which will open only when authorized user will tag to open the door. It is been illustrated in Fig. 2. Once a correct tag is entered the current position of the user will be in the secondary security circle. If the correct fingerprint is scanned by the sensor correct, then the danger message will not be altered is via the GSM module. The GSM module, alerts the authorities, if the protocol, are picked without the goods. Fig. 3 represents the inner security loop with the flow of the events occurring.

C. Secondary Circuit Diagram:

All the sensor connections are shown in Fig. 4. The prototype model is written based on the above circuitry. Each And every sensor is connected. Along with the processor and is given VCC and GND supply. All the different type of sensor requires different number of input. Hex Keypad has eight input ports and the fingerprint module has two.

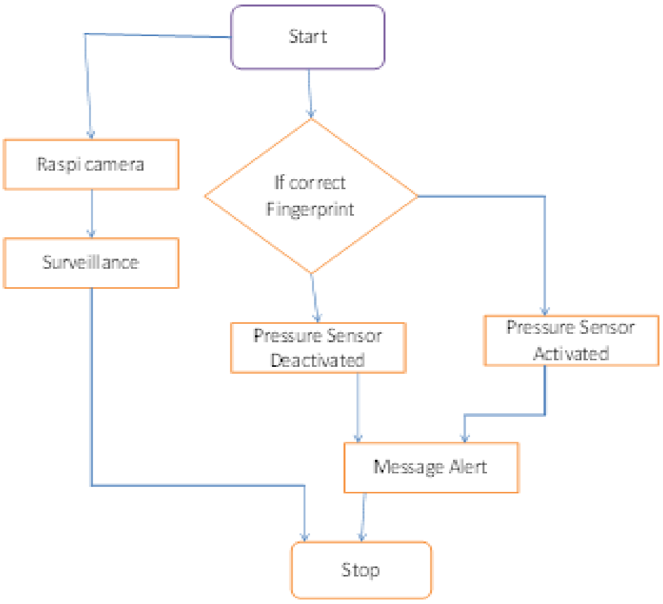


Fig. 3: Flow chart for Secondary Circuit.

III. DESIGN AND IMPLEMENTATION

A. Hex Keypad:

Hex Keypad is the primary security to walk into the premises, in multi-level security systems. Below figure show the 4*4 hex keypad security systems (Fig 4). It will open only when the correct password is entered, rotates the motor for opening the door. If the sequence of pressing the keys is mismatched from the already existing or set pattern, the door will be locked. The specifications are displayed in the below table.

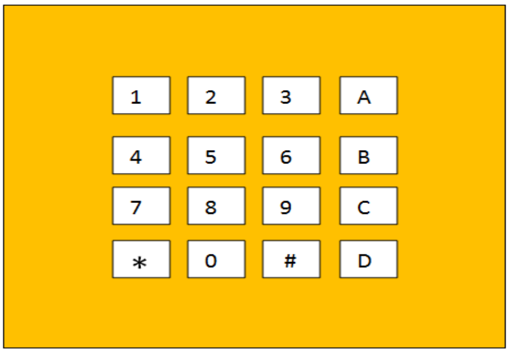
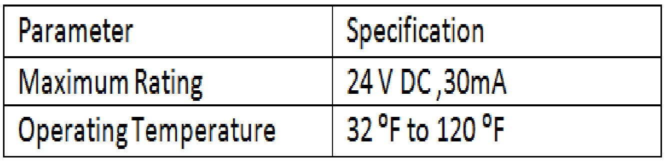


Fig 4: Hex keypad.

TABLE 1: HEX KEYPAD



Parameter	Specification
Maximum Rating	24 V DC ,30mA
Operating Temperature	32 °F to 120 °F

B. Bluetooth:

The next stage of security system is done by wireless mechanism, using Bluetooth signals. A Bluetooth device HC 05 is placed near the door. When a person enters premises, the user, types in the security code through a mobile phone application which, if correct, opens the motor via the microcontroller or the door remains closed. Assuming the fact that the authorized user knows the code then it is a guaranteed approach of maximum security.

C. RFID:

The third level of security system has RC522 RFID tag system. Each tag consists of unique identity number which is already pre-coded in the system. As the registered RFID tag is sent near to the receiver (Fig. 5), the code for the particular tag is matched to the pre-registered code stored in the system and the signals will be sent to the actuator to perform specific work. If the unauthorized user tries to assess the code and if the code does not match then the actuator does not receive any signal. As each of the RFID tag has a unique identity, therefore each time a tag is used to enter into the safe; the key can be rotated with the person who is authorized user with that specific tag from the logs in the system.

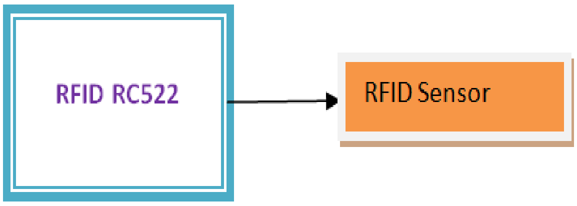


Fig. 5: Radio frequency identification.

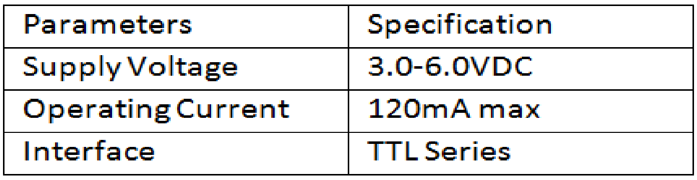
D. Pressure Sensor:

An array of pressure sensors are placed under the valuables when the object is removed from its original place, a signal will be sent to the processor, which alerts the authorities of the users. The pressure sensors are deactivated only when the authorized user fingerprint is scanned on the fingerprint scanner, allowing the goods to be accessed with ease

E. Fingerprint Sensor:

After passing through the three checkpoints, the last and the final security that is available in the system is a fingerprint scanner R305. The main key point of the scanner is that it is being attached to a secondary processor unit and it is provided with a separate supply. In order to access the valuable item, allows only to the top officials of their fingerprint that has been scanned. As the key is matched, the pressure sensor is deactivated and allows the good to access. The key point of attaching the fingerprint sensor system is not only to get into inside the premises but also for accessing the good by the authorized user only. A scanner system is shown in Fig. 7 with the specifications for the fingerprinting operation in Table 2.

TABLE 2: FINGERPRINT SCANNER



Parameters	Specification
Supply Voltage	3.0-6.0VDC
Operating Current	120mA max
Interface	TTL Series

F. GSM Module:

A GSM SIM900 module is connected to the secondary security unit. The module is grouped into two with the microprocessor Raspberry Pi. The all type of SIM card that are working can be put into the module for making it user friendly. The functioning of the module is such that, when the goods from the inner room that had to be accessed without the correct protocol, the above module will sends out alert messages to the authorized user for the required action to be taken. If the correct protocols are followed, the message alert is sent, so that the information can be recorded correctly.

G. Raspberry Pi Camera:

This Raspi Camera that is used in the above model is used mainly for the online streaming. Connected with a Raspberry Pi is shown in Fig. 6. Online Streaming in the innermost circle is done mainly by using Raspberry pi processor that can be viewed by typing the IP address of the host in any web server.

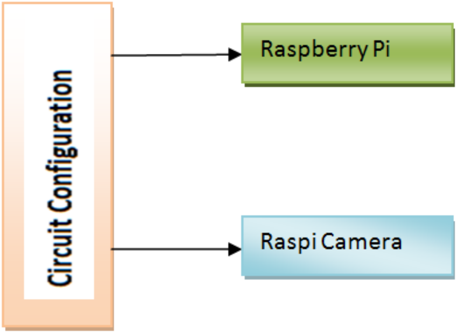


Fig 6: Raspi camera.

H. Software:

Raspbian Operating system is loaded mainly on the SD card with the NOOBS OS which is necessary part of the Raspberry pi. The coding of the sensors part and modules that are attached to the raspberry pi is done on the python platform. Mainly coding on python can be done by using the shell and by python software that is IDLE.

TABLE 3: COMPARISON OF SENSORS

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

IV. LITERATURE SURVEY

As per the current survey there exists no system at lesser rates. Some of the systems are hard to install, hard to use and maintain. Current systems are generally proposed and closed, but not very customized by the end user.

1. N. Sriskanthan explained the model for home automation using Bluetooth via PC. But the system lacks to support mobile technology.

2. Muhammad IzharRamli [2] designed a device called prototype electrical device using Web. They also set the server with a auto restart if the server condition is low.

3. Hasan [5] has developed a device called telephone and PIC remote controlled for controlling the devices pin check algorithm that has been introduced where it was a cable network but not wireless communication.

4. Pradeep G [4] had proposed home automation system using Bluetooth device which saves lot of power and time using technique to save the preloaded list by not making it to setup connection all the time when required.

5. Al-Ali and Al-Rousan [3] has presented a design and implementation technique using a Java-based automation system through World Wide Web. It had a standalone embedded system board integrated into a PC-based server at home.

6. AmulJadhav [6] designed an application in a universal XML format which can be easily transformed to any other mobile devices rather than pointing to a single platform.

V. CONCLUSION

The gain of multi-level security is observed in the above model, which consists of two different mechanisms to reach the vault, powered by different powering units. The primary system consists of the Hex Keypad, Bluetooth module and the RFID. All the primary system is coded password, which are accessible by the authorized person who has the clarity to enter into the next level as shown in. Fig. 7 which shows Primary Level of Security that is working on the first protocol. The secondary security system, works on a second protocol that is in terms with accessing the goods that are stored inside the vault.

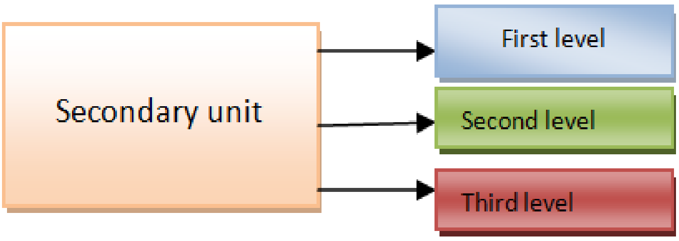


Fig 7: Model of Primary level of Security

REFERENCES

[1] D. Javali, M. Mohsin, S. Nandanwar, and M. Shingate, "Home automation and security system using Android ADK," *Int. J. Electron. Commun.Comput. Technol.*, vol. 3, no. 2, pp. 382–385, Mar. 2013.

[2] V. K. Sadagopan, U. Rajendran, and A. J. Francis, "Anti theft control system design using embedded system," *Proc. IEEE*, Jul. 2011.

[3] R. Piyare, "Internet of Things: Ubiquitous home control and monitoringsystem using Android based smart phone," *Int. J. Internet Things*, vol. 2,no. 1, pp. 5–11, 2013.

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet ofThings: Vision, applications and research challenges," *Ad Hoc Netw.*,vol. 10, pp. 1497–1516, Sep. 2012.

[5] P. Vigneshwari, V. Indhu, R. R. Narmatha, A. Sathinisha, andJ. M. Subashini, "Automated security system using surveillance," *Int.J. Current Eng. Technol.*, vol. 5, no. 2, pp. 882–884, Apr. 2015.

[6] K. Gopalakrishnan, V. S. Kumar, and G. Senthilkumar, "Embeddedimage capturing system using raspberry pi system," *Int. J. Emerg. TrendsTechnol. Comput. Sci.*, vol. 3, no. 2, pp. 213–215, Apr. 2014.

[7] S. Prasad, P. Mahalakshmi, A. J. C. Sunder, and R. Swathi, "Smartsurveillance monitoring system using raspberry PI and PIR sensor," *Int.Comput. Sci. Inf. Technol.*, vol. 5, no. 6, pp. 7107–7109, 2014.

[8] D. Shah and V. Bharadi, “IoT based biometrics implementation on raspberry Pi,” *Proc. Comput. Sci.*, vol. 79, pp. 328–336, Mar. 2016.

[9] P. Kumar and P. Kumar, “Arduino based wireless intrusion detectionusing IR sensor and GSM,” *Int. J. Comput. Sci. Mobile Comput.*, vol. 2,no. 5, pp. 417–424, May 2013.

[10] A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smarthome automation system,” *Future Generat. Comput. Syst.*, vol. 56,pp. 719–733, Mar. 2016.

[11] N. K. Sonawane, P. D. Wwaghchavre, and K. A. Patel, “Bluetooth baseddevice automation system using cellphone,” *Int. J. Comput. Appl. Inf.Technol.*, vol. 7, no. 1, pp. 136–141, Oct./Nov. 2014.

[12] S. Kumar, “Ubiquitous smart home system using Android application,”*Int. J. Comput. Netw. Commun.*, vol. 6, no. 1, pp. 2–3, Jan. 2014.

[13] A. C. Sari, A. Rahayu, and W. Budiharto, “Developing informationsystem of attendance and Facebook status for Binus University’s lecturerusing raspberry pi architecture,” *Proc. Comput. Sci.*, vol. 59,pp. 178–187, Mar. 2015.

[14] M. N. Jivani, “Gsm based home automation system using app-inventorfor Android mobile phone,” *Int. J. Adv. Res. Elect., Electron. Instrum.Eng.*, vol. 3, no. 9, pp. 12121–12128, Sep. 2014.

[15] V. Vujovi´c and M. Maksimovi´c, “Raspberry pi as a sensor Web nodefor home automation,” *Comput. Elect. Eng.*, vol. 44, pp. 153–171,May 2015

[16] N. Sriskanthan and Tan Karand. “Bluetooth Based Home Automation System”. *Journal of Microprocessors and Microsystems*, Vol. 26, pp.281-289, 2002.

[17] Muhammad IzharRamli, MohdHelmyAbdWahab, Nabihah, “TOWARDS SMART HOME: CONTROL ELECTRICAL DEVICES ONLINE” ,Nornabihah Ahmad International Conference on Science and Technology: Application in Industry and Education (2006).

[18] Muhammad IzharRamli, MohdHelmyAbdWahab, Nabihah, “TOWARDS SMART HOME: CONTROL ELECTRICAL DEVICES ONLINE” ,Nornabihah Ahmad International Conference on Science and Technology: Application in Industry and Education (2006) .

[19] Pradeep.G, B.Santhi Chandra, M.Venkateswarao, “Ad-Hoc Low Powered 802.15.1 Protocol Based Automation System for Residence using Mobile Devices”, Dept.of ECE, K L University, Vijayawada, Andhra Pradesh, India IJCST Vo l. 2, SP 1, December 2011 .

[20] E. Yavuz, B. Hasan, I. Serkan and K. Duygu. “Safe and Secure PIC Based Remote Control Application for Intelligent Home”. *International Journal of Computer Science and Network Security*, Vol. 7, No. 5, May 2007.

[21] AmulJadhav, S. Anand, NileshDhangare, K.S. Wagh “Universal Mobile Application Development (UMAD) On Home Automation” MarathwadaMitraMandal’s Institute of Technology, University of Pune, India Network and Complex Systems ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol 2, No.2, 2012 .

[22] Rana, JitendraRajendra and Pawar, Sunil N., Zigbee Based Home Automation (April 10, 2010). Available at SSRN: http://ssrn.com/abstract=1587245 or http://dx.doi.org/10.2139/ssrn.1587245.

[23] R.Piyare, M.Tazil” Bluetooth Based Home Automation System Using Cell Phone”, 2011 IEEE 15th International Symposium on Consumer Electronics.

[24] S. Sivaranjani and Dr. S. Sumathi, Implementation of Fingerprint and Newborn Footprint Feature Extraction on Raspberry Pi, IEEESponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS’15.

[25] Kaul, V.; Bharadi, V.A.; Choudhari, P.; Shah, D.; Narayankhedkar, S.K,” Security Enhancement for Data Transmission in 3G/4G Networks”,IEEE sponsored 1st International Conference on Computing, Communication, Control, and Automation (ICCUBEA), February 2015, pg. 95– 102.