Smart Home Safety Device using Frequency Hopping approach based on GSM Generation

Neha R. Ghate[1] K.V.Kale[2]
Department of Computer Science & Information Technology
Dr. Babasaheb Ambedkar Marathwada University Aurangabad, Maharashtra, India

Abstract— *The reliable, real-time, verbal exchange is crucial to the success of army operations. Because of the highly transitional nature of the theater of operation, wire line communiqué is often no longer feasible, so wireless conversation systems ought to be deployed as an alternative. Furthermore, the deployment must often be completed hastily, without the luxurious of careful coverage planning and evaluation to be had whilst putting in civilian mobile networks. As an end result, army wireless communiqué systems present challenging communiqué surroundings, needing to cope with impairments along with channel fading, interference and jamming, while also addressing safety issues.*

Keywords— PIC18F452 Microcontroller, GSM Module, RF Module, Frequency Hopping Method

I. INTRODUCTION

A. Embedded System

1) Definition:

An Embedded System is a system that has embedded software and computer hardware, which makes it a system dedicated for an application or a specific part of an application or product or a part of a larger system. [1]

2) Microcontroller:

A microcontroller is an integrated chip that has processor, memory and several other hardware units in it; these from the microcomputer part of the embedded system. [2][3]

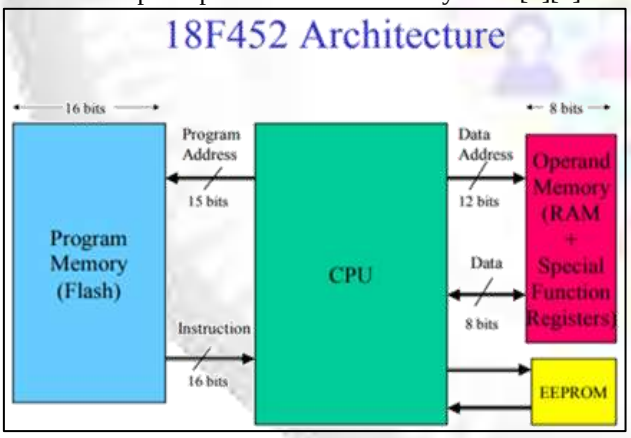

Fig. 1: Architecture of PIC18F452

The PIC Processor has Harvard architecture –i.e. separate instruction memory and data memory. [4]

- For the 18F452: – 32KByte Program Memory on chip, (Flash) – 1792 bytes of Data Memory on chip
- 1536 bytes of static RAM
- 256 bytes of EEPROM

II. OBJECTIVE

Smart domestic safety System will work on Wi-Fi communications and cutting-edge mobiles for the safety machine. The traits of the clever home safety device that includes remote controlling of appliances, intrusion detection, and system safety and vehicle-configuration such that machine mechanically adjusts the machine settings on running hardware help take a look at. [5]

The principal objectives of the home protection gadget are as comply with:

- Statuses are displayed on LCD to signify the state of the gadget.
- With Keypad for smooth interplay with the device.
- Security machine with OTP safety. Number storing/analyzing is best completed if and simplest if OTP (one time password) is matched that's dispatched to predefined wide variety as while required to Store/ examine/any saved numbers or to trade any settings. This function increases the robustness of system against any hacking tries to exchange/examine saved numbers or settings.
- System ON/OFF times are stored, which can be retained every time required. This will assist one to realize the variety of instances the gadget becomes switched off. [6][7]

III. LITERATURE SURVEY

A. How the Concept of Security has changed inside the Modern Home

"The responsibilities of a modern-day safety gadget consist of figuring out an interloper seeking to advantage get entry to the house, alerting the owner of a house approximately the intrusion or intrusion strive, preventing the intruder from gaining access to the home, and collecting or collecting proof concerning the intrusion so that the perpetrators may be brought to justice." The development of era has contributed to the converting concept of safety in modern-day homes. It has changed from an easy lock and key safety idea to enforcing state-of-the-art protection structures the usage of cameras, microphones, contact sensors, proximity sensors, alarms, silent alarms, and so forth. By connecting present-day houses to the Internet which could be very popular these days, customers can get entry to and manipulate their homes remotely at any time and from anywhere in the world.[8]

A growth in processing power of newly-designed processors and the massive reduction in energy intake, fee, and length of latest electronics devices allow people to know and manipulate each thing of their home, like which door or window is open, which tool or mild is switched on, and which rooms are occupied. Inhabitants can maintain a watch on their domestic the use of stay video and audio feeds from distinct parts of their domestic. They can also be aware of exclusive environmental factors inside and outside their domestic, like humidity, temperature, and light intensity. In a Wireless Sensor-Actor Network, sensors gather information about the physical global or surroundings around them. Actors perform the proper movements on the

surroundings as directed by means of the consumer or every other birthday celebration. Improvements in Wireless Sensor Actor Networks are certainly a contributing issue within the popularity of clever homes. [9]

Combining Ubiquitous Computing, Wireless Sensor Actor Networks and the popularity of the Internet has allowed designers, engineers, and researchers to give you green techniques to allow home inhabitants to get entry to and manipulate each and every component of their domestic, inclusive of the surroundings. [10][11]

B. Various Home Automation Methodologies Analyzed from a Security Standpoint

1) Context-aware Home Automation Systems:
A contemporary home may be accessed with the aid of its inhabitants from the outdoor thru Internet, Global System for Mobile verbal exchange (GSM), and wireless portable devices like cellular phones, capsules, laptops, or through desk-bound devices like a workplace laptop (PC). [12]

2) Central Controller-based totally Home Automation System:
A valuable controller-based home safety machine looks to enhance the security of the houses in a locality through combining many houses into a safe community with a control node devoted for every locality depending on the number of customers. These manipulate nodes are controlled by using a few important or leader manage nodes with drastically high processing power. The safety device defined via S. Tsai et al, known as Home Security System on Intelligent Network (HSSIN), and uses this kind of primary controller-primarily based technique. The proposed device lacks present-day security parameters. [13]

3) Bluetooth-based totally Home Automation System:
The work of N. Sriskanthan et al.Suggests the implementation of a domestic automation system the usage of Bluetooth. They use a bunch controller applied on a PC, that's connected to a microcontroller-based totally sensor and tool controllers. The researchers even built a brand new protocol on top of the Bluetooth software program stack, referred to as Home Automation Protocol (HAP), to make the communiqué between gadgets viable. The tool controller is hooked up to digital gadgets thus the I2C Bus. The device allows more than one device controller to be linked to the host controller. [14]

4) GSM or Mobile-based Home Automation System:
Mobile-based totally domestic automation is attractive to researchers because of the recognition of cellular phones and GSM generation. We especially remember 3 options for verbal exchange in GSM, particularly SMS-based home automation, GPRS-primarily based home automation, and Dual Tone Multi-Frequency (DTMF)-based totally home automation. Each of that three technology is mentioned below, in conjunction with their shortcomings. [15]

5) SMS-based Home Automation System:
The proposed gadget detects unlawful intrusions at domestic and permits valid users to alternate the passkey for the door and manage lights inside the domestic. The unlawful intrusion into the house is recognized by using tracking the kingdom of the home door, that is performed the usage of Light Emitting Diode (LED) and infrared sensors. [16]

6) GPRS-primarily based Home Automation System:
There is a variety of domestic safety systems carried out the use of GPRS. Most systems use the phrase security inside the conventional feel, and simplest cope with the danger put forth by means of old-school intruders in domestic. [17]

7) DTMF-primarily based Home Automation System:
The work of L. Muhury and A.H.M.A Habib describes the design and implementation of a DTMF-based totally domestic automation device. The consumer calls a SIM range assigned to the home and presses the digits on their telephone's keypad to govern the home's gadgets with the aid of generating a DTMF tone. The tone is acquired and decoded through the GSM module at domestic the usage of a DTMF decoder. The decoded instructions are passed to the microcontroller in order that user commands can be implemented at domestic. [18]

8) Internet-based Home Automation System:
Internet or IP protocol-based totally conversation in home automation systems is usually a famous desire among researchers. The Internet is without difficulty scalable, bendy on the subject of get entry to and use, and really famous as a communiqué technique in today's world, so the hardware and the community required forget right of entry to is without problems to be had, gives excessive bandwidth and very low communiqué cost, and devices can connect with and disconnect from the network without problems. [19]

9) Decentralized Approach to Home Automation Systems:
Home automation structures discussed thus far use a valuable controller or centralized approach, which has a single point of failure. [20]

10) Role of User Interface in Security:
According to a recent examine completed on cellular telephone utilization, by means of the stop of 2017, 13 billion people will be the use of cellular phones, and out of them, 2.50 billion might be using smart phones. It is handiest a natural evolution for humans to assume more functionality on their telephones, like controlling their homes from it. User interfaces provide a way for a user to interact with software, in this example their domestic automation device. So, understanding a consumer's possibilities and the way a user interacts with a tool is important in making sure home safety. [21]

IV. METHODOLOGY

A. PIC Microcontroller

Microcontroller is a tool that uses a specific code to perform all tasks and control of all home devices. We used "PIC" microcontroller as the central controller unit of the system has many features that support our project, (like2 PWM 10-Bit flash type of program memory 32 KB program memory and other features see datasheet.

- Data RAM serves the role of registers and main memory – i.e. there is no distinction between data accesses to registers and memory – Can think of the processor as having lots of registers and no additional data memory. [22]

B. PIC Program Memory

- 215 = 32K = 32768 program memory locations (bytes).

- Most PIC instructions occupy two bytes (a few occupy 4 bytes).
- CPR can read two bytes at a time from Program memory.
- This is non-volatile flash memory in the 18F452. – Can be read (in 8 or 16 bit units) at processor speed – Limited write/erase ability.

C. PIC (RAM) Data Memory:

- 12 data address bits allow for 212 = 4K = 4096 data memory locations (bytes). – PIC 18F452 implements only 1536 bytes of data memory
- This is volatile static RAM memory which can both be read and written.
- The non-volatile EEPROM data memory is accessed via a separate mechanism. – EEPROM can be read at near processor speed – Can be written to in byte units – Write times are MUCH slower (measured in msec)

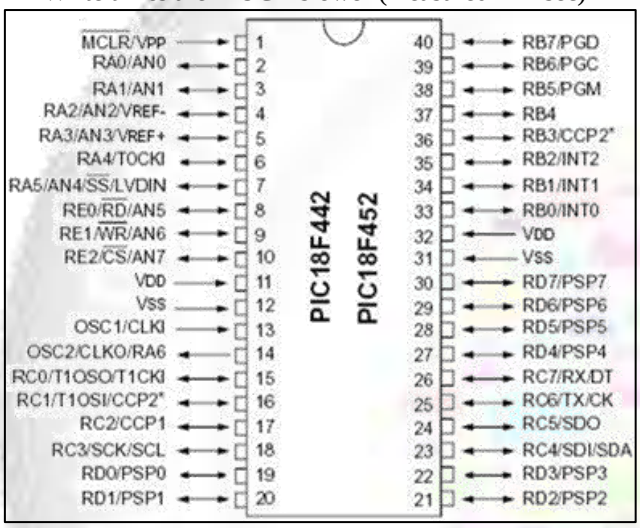

Fig. 2: Pin Diagram of PIC18F452

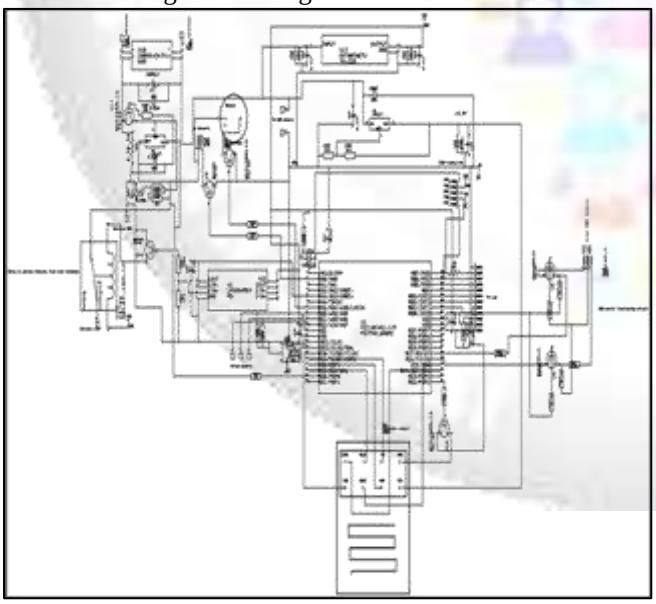
Fig. 3: Shematic Representation

According to schematic, L7805 is used to convert high voltage ~15V from charger circuit to 5V for PIC. PIC's PORTB is used for LCD communication. And U5 is used to decrease 5V to ~3V used by NRF. Two NPN transistors are used as a switch one for buzzer and one for Hooter. Small relay is used to switch charging of battery. Resistors R21 and R22 acts as a voltage divider to divide high voltage from battery to low voltage (0 to 5V) for PIC ADC. U2 is an OPAMP as a buffer to decrease impedance towards PIC Input pin. Resistors R40, R32, R35, R34, R41, R31, U8, U9 acts a level shifter required for interfacing PIC UART with SIM900 via TTL interface. In it GTX indicate GSM TX pin and GRX indicates GSM RX pin IC microcontrollers are a family of specialized microcontroller chips produced by Microchip Technology in Chandler, Arizona. The acronym PIC stands for "peripheral interface controller," although that term is rarely used nowadays. A microcontroller is a compact microcomputer designed to govern the operation of embedded systems in motor vehicles, robots, office machines, medical devices, mobile radios, vending machines, home appliances, and various other devices. A typical microcontroller includes a processor, memory, and peripherals. [23][24]

Every PIC microcontroller has a set of registers that also function as RAM (random access memory). Special purpose control registers for on-chip hardware resources are also mapped into the data space. Every PIC has a stack that saves return addresses. The stack was not software-accessible on the earlier versions of the PIC, but this limitation was removed in later devices. [25][26][27]

V. RESULT

In this research, the System will works on wireless communications and latest mobiles for security purpose. The main advantage of this system to system security, intrusion detection, involves remote controlling of appliances and auto configuration such that system automatically adjusts the system settings on running hardware support check. This research is mainly used for security purpose; no one can operate this system without OTP matching.

Due to the explosive global growth in the number of mobile subscribers, as well as the growth predicted inside the cell data phase, the want for stepped forward spectrum efficiency on the radio interface will become increasingly critical. Frequency hopping (FH) is an effective technique for improving the spectrum performance. One of the benefits of FH is that it is able to be combined with other spectral efficiency improving functions like energy manipulate, handover and reuse partitioning Performance Enhancements in a Frequency Hopping GSM Network covers FH and a few of the extra capabilities in detail. It starts off evolved with an in-intensity description of the basic idea of FH on link level in addition to on machine degree. Different strategies have been used for analysis, consisting of hyperlink degree simulations, community stage simulations and traditional tele-site visitor's idea

VI. CONCLUSION

Our work specializes in the safety factor of the prevailing domestic automation system and factors out its flaws. It indicates how the idea of protection and that means of the word "intruder" have modified in current homes. The paper factors out the shortcomings of current home automation structures in figuring out and stopping sophisticated intruders in a domestic environment. For future paintings

inside the discipline of domestic automation protection, we encourage the researchers to don't forget a domestic automation gadget as an entire and increase behavior prediction and superior sensing parameters that could help to perceive and save you professional and complex intruders. Security is vital for the proper implementation and development of the house automation structures. Moreover, it affords a sense of security to a home's population and puts their minds cozy.

ACKNOWLEDGMENT

This work is supported by Department of Science and Technology under the Funds for Infrastructure under Science and Technology (DST-FIST) with sanction no. SR/FST/ETI- 340/2013 to Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. I am thankful to "SAP lab" and "UNIVERSITY GRANTS COMMISSION" for providing me "Post¬ Graduate Scholarship for Professional Courses for SC/ST Candidates 201516".The authors would like to thank Department and University Authorities for providing the infrastructure and necessary support for carrying out the research.

REFERENCES

[1] Veena A. Patil Asst. Prof. Department. of Computer Science and Engineering BLDEA's Dr. P. G. H CET Vijayapur," SMART LOCK", International Journal of Engineering Applied Sciences and Technology, 2016.

[2] Mrinal Mile, Priyanka Lakade, Saniya Mashayak, A. B. Gavali, Department of Computer Science and Engineering, SPVP's S.B. Patil College of Engineering, SPPU, Indapur, Pune, India, Design of "Smart Home Automation System using Android Application, Journal of Android and IOS Applications and Testing" Volume 2 Issue 1,2017.

[3] Bhagyashri Tembhare1, Triveni Meshram2, Ashwini Meshram3, Punam Panchbhai4, Prof-Deepali Nirvikar5 Department of Electronics and Communication Engineering MIET, Shahapur Bhandara, MH-441904," Automated Security System " International Journal of Research in Applied Science & Engineering Technology" (IJRASET), Volume 5 Issue III, March 2017.

[4] Madhusagar. S1, Murthy. M2, Deepak. G3," Intelligent and Advance Home Security "System to Lock and Unlock using Mobile Phones", International Journal of Engineering Trends and Technology (IJETT) – Volume 37 Number 7 - July 2016.

[5] Shreyas V, Mohanraj N, Vishal Chandra R, Bhargav Bellur Department of Electronics and Communication Engineering PES University," Effective Home Security leading to Access Control Solutions in Smart Cities", International Journal of Engineering Trends and Technology (IJETT) July 2016.

[6] Ratnamala Prakash More1, Prof. Dr. Anil. S. Hiwale, "A Reconfigurable Smart Sensor Interface for Industrial WSN in IoT Environment", International Journal of Innovative Research in Science, Engineering, and Technology, Vol. 5, Issue 5, May 2016.

[7] Nidhi Gau, Shabarinath B.B, Design and "Implementation of Home Monitoring System Using RF Technology", International Journal of Advances in Electrical and Electronics Engineering, International Journal of Advances in Electrical and Electronics Engineering, Vol. 6, Issue 6, May 2016.

[8] Arun Cyril Jose and Reza Malekian, Smart "Home Automation Security: A Literature Review", Smart Computing Review, vol. 5, no. 4, August 2015

[9] F. Shawki1, 2, M. El-Shahat. Dessouki1,3, A. I. Elbasiouny4, A.N. Almazroui5, F. M. R. Albeladi5, "MICROCONTROLLER BASED SMART HOME WITH SECURITY USING GSM TECHNOLOGY", IJRET, published on 04 Issue: 06 | June-2015.

[10] Renuka P. Dhage1, S.P.Kharde , A Review on Home Automation System (HAS), "International Journal of Advanced Research in Electrical, Electronics and Instrumentation", Engineering, Vol. 4, Issue 10, October 2015

[11] 11. Sougata Das Department of ECE, University Institute of Technology, University of Burdwan, Golapbag, "Embedded System for Home Automation Using SMS", IEEE International Conference on Automation, Control, 2014 IEEE.

[12] The-History-of-Home-Security 4th July 2010 [Online]. Available: http://ezinearticles.com.

[13] V. Karri and J. S. Daniel Lim, "Method and Device to Communicate via SMS after a Security Intrusion", 1st International Confe-rence on Sensing Technology, Palmerston North, New Zealand, (2005) November 21-23.

[14] Y. Zhao and Z. Ye, "Low cost GSM/GPRS BASED wireless home security system", IEEE Trans. Consumer Electron, vol. 56, no. 4, (2007) January, pp. 546-567.

[15] Z. Bing, G. Yunhung, L. Bo, Z. Guangwei and T. Tian, "Home Video Security Surveillance", Info-Tech and Infonet, 2001,Proceedings,ICII 2001-Beijing. 2001 International Conference, vol. 3, pp. 202-208.

[16] M. Meyer, M. Hotter and T. Ohmacht, "A new system for Video-based Detection of moving objects and its integration into digital networks", Security Technology 1996, 30th Annual 1996 International Carnahan Conference, (1996), pp. 105-110.

[17] Mae , Y,; Sasao , N .; INNoue ,K. ; Arai,T.; "Person Detection by Mobile Manipulator for Monitoring",SICE 2003 Annual Conference, pages-2801-2806.

[18] "SMS Based Wireless Global Range Automation & Security System", Sudipan Saha, Sutasom Bhaumik.

[19] "Analysis and Performance of a Low Cost SMS Based Home Security System", Sheikh Izzal Azid, Sushil Kumar, International Journal of Smart Home, vol. 5, no. 3, (2011) July.

[20] M. Butt, M. Khanam, A. Khan, M. Sikandar and H. Khiyal, "Controlling Home Appliances Remotely Through Voice Command", (IJACSA) International Journal of Ad-vanced Computer Science and Applications, Special Issue on Wire-less & Mobile Networks, pp. 35-39.

[21] N. Sklavos, P. Kitsos, O. Koufopavlou, "VLSI Design and Implementation of Homophonic Security System", proceedings of IEEE Computer Society Annual

Symposium on VLSI (IEEE ISVLSI'12), Amherst, USA, August 19-21, 2012.

[22] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon, "Home automation in the wild: challenges and opportunities", proceedings of the SIGCHI Conference on Human Factors in Computing Systems '11, ACM, USA, 2011.

[23] N. Sklavos, "Cryptographic Hardware & Embedded Systems for Communications", proceedings of the 1st IEEE-AESS Conference on Space and Satellite Telecommunications, Rome, Italy, October, 2-5, 2012.

[24] R.A.Ramlee, M.H.Leong, R.S.S.Singh, M.M.Ismail, M.A. Othman, H.A. Sulaiman, M.H. Misran, M.A. Meor Said, "Bluetooth Remote Home Automation System Using Android Application", The International Journal of Engineering And Science, Volume 2, pp. 149-153, January 2013.

[25] Vini Madan, S.R.N Reddy, "GSM-Bluetooth based Remote Monitoring and Control System with Automatic Light Controller", International Journal of Computer Applications, Volume 46-No.1, May 2012.

[26] B.Suresh Babu, Dr. C. Venkata Narasimhulu, "Robust Model to Access Consumer Appliances Using Android", International Journal of Research in Advent Technology, Vol.2, No.10, October 2014.

[27] Somak R. Das, Silvia Chita, Nina Peterson, Behrooz A. Shirazi, Medha Bhadkamkar, "Home Automation and Security for Mobile Devices", Ninth Annual IEEE International Conference on Pervasive Computing and Communications, March 2011