ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/330472779

Design of an Improved Cost Effective Electronic Locking System

Conference Paper · November 2018

DOI: 10.1109/IEMCON.2018.8614749

CITATIONS
3

READS
280

6 authors, including:

Happy Nkanta Monday
Oxford Brookes College of Chengdu University of Technology
50 PUBLICATIONS **574** CITATIONS
SEE PROFILE

Grace U. Nneji
Oxford Brookes College of Chengdu University of Technology
48 PUBLICATIONS **447** CITATIONS
SEE PROFILE

Chiagoziem Chima Ukwuoma
University of Electronic Science and Technology of China
61 PUBLICATIONS **556** CITATIONS
SEE PROFILE

All content following this page was uploaded by Happy Nkanta Monday on 07 January 2022.

The user has requested enhancement of the downloaded file.

Design of an Improved Cost Effective Electronic Locking System

Happy N. Monday
School of Computer Science and Technology
University of Electronic Science and Technology of China
Chengdu, China
mh.nkanta@gmail.com

Jian P. Li
School of Computer Science and Technology
University of Electronic Science and Technology of China
Chengdu, China
jpli2222@uestc.edu.cn

Grace U. Nneji
School of Information and Software Engineering
University of Electronic Science and Technology of China
Chengdu, China
ugochinneji@gmail.com

Chiagoziem C. Ukwuoma
School of Information and Software Engineering
University of Electronic Science and Technology of China
Chengdu, China
chiagoziemchima@gmail.com

Ifeanyi D. Dike
Department of Mathematical Sciences
School of Sciences
Federal University of Technology, Akure
Ondo State, Nigeria
lorddickson751@gmail.com

Richard I. Nneji
Department of Chemical Engineering
School of Engineering
University of Lagos, Akoka
Lagos, Nigeria
richardnneji89@gmail.com

***Abstract*— the design of an intelligent electronic safe provides a better way of ensuring the security and safety of data. The use of microcontroller as an embedded technology in controlling date is desirable to implement a lock mechanism to solve man's problems in homes, offices and regular automobiles. This paper proposes a design of an improved cost effective electronic locking system which restricts access to certain important data and valuables to certain individuals. The electronic safe prompts the user or access seeking person for certain security data, processes the data and takes logical decisions which leads to the granting of access or denying of access to restricted safe. The most important strength of the system is the ease with which a user can easily change personal access key without contacting any professional or programmer. The system removes emphasis from mechanical mechanisms for protection of valuable properties and emphasized on the strength of keyless electronic locks.**

Keywords*— *Microcontroller, electronic lock, cost, security, system design, implementation

I. INTRODUCTION

Safes have existed in various forms for thousands of years. As with locks, it wasn't until the late 1700s that security became the primary concern. Jason Johnson and Yves Behar designed a keyless entry system with any Bluetooth-enabled smart-phone called August lock [1]. When a registered device gets near to the lock the homeowner or visitor can open the door by pressing the relevant address entry on the August app. The problem with the system is the limited security it presents; anyone with the august-mobile app would easily access the system. Also, convenient digital door lock a function, such as remote control via the integration of mobile devices and key sharing was investigated [2]-[4]. A method for detecting, accessing and transmitting the object image was proposed [5], [6]. A method for opening and closing the door lock using voice recognition, without using a network was presented in [7], [8]. A security system that interfaces with an Android mobile device was proposed in [9], [10]. The mobile and security system communicate via Bluetooth in a short range was investigated in [11]. An application was developed for communication between devices for transferring the state of the alarms generated in a home through a door lock in the neighborhood [12]. Face recognition for the door lock open is available in literature as well [13]-[15]. In particular, an application method that transfers the SMS about the legitimacy of the user to the mobile device was proposed in [16]. These systems are all novels but have one common pitfall; the door drive is powered by A.C electric energy. Security applications for home automation are presented in [17]-[20]. It is shown by initial studies that remotely controlling a door lock cannot be classified also into application of the complete IoT [21]-[23]. The methods mentioned above strengthen the security functions. These systems are limited because the owner has to use a platform to access the system. Security of human life and property is one of the paramount challenges facing our contemporary society [24], [25]. The design and implementation of an intelligent electronic safe provides a sure way of ensuring the security and safety for data [26]-[28]. The proposed system in this paper doesn't need any mobile platform for its control nor does it need any form of app which must be used to control it. Also, it uses D.C power supply whose availability can be sufficiently guaranteed. Furthermore, the system allows the owner to reset the pass-code in event of someone accidentally seeing it.

A. Analysis of the Existing System

There are various differing security lock systems in use today with slight differences in their design and performance. The old systems or means of securing lock usually involve using knobs and bolts to lock and secure properties.

978-1-5386-7266-2/18/$31.00 ©2018 IEEE

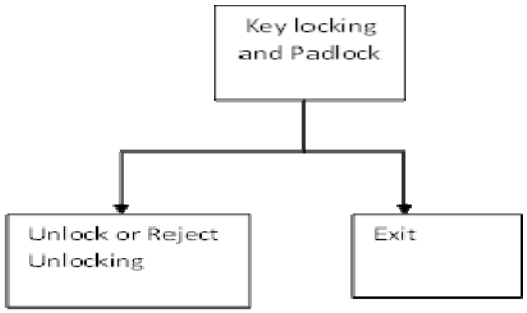

Fig. 1. High Level Model of the Existing System

B. *Problems of the Existing System*

The problems associated with the existing system of security locks are:

- Inability to operate automatically; the lock has to be manually opened and pushed by the prospective door user.
- Physical Keys and un-lockers are always needed. Often, losing the key would inevitably result to breaking the door or lock.
- Inefficiency: the system is not optimal in its operation. Sometimes, rust may affect the locks and prevent them from having optimal performance.
- Higher aggregate cost; the structure, complexities, and regularities of failures of the system ensure that the accrued cost of the system is increased.
- High cost of construction. They are more expensive in implementing.

II. Analysis of the Proposed System

The different sections interact to ensure a working coded lock security system. When the keys of the button on the input port are pressed, different numeric values are generated and displayed on the screen. By clicking the select button, the number on the screen is selected and moved into the temporary memory (accumulator). When the enter button is pressed, the microcontroller access the temporary memory and compares its content with a particular dedicated code. The system is designed in such a way that the system grants access to a potential user and the sliding door opens whenever the codes are the same buttons but denies access to the user whenever they differ. In describing the operation of the system, a block diagram has been developed as shown below:

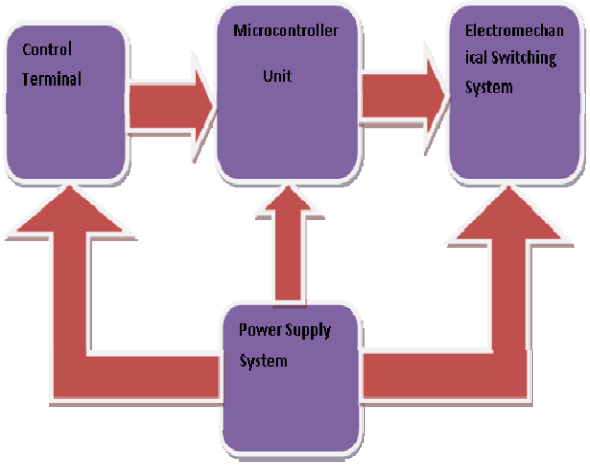

Fig. 2. Block Diagram of Component of the System

A. *Model of the Proposed System*

The system constitutes of the following sub-units: control terminal, microcontroller, regulated power supply and electromechanical switching interface. They are systematically interfaced and made to intercommunicate. For good understanding of the system, a good look at the section which constitutes the system becomes imperative.

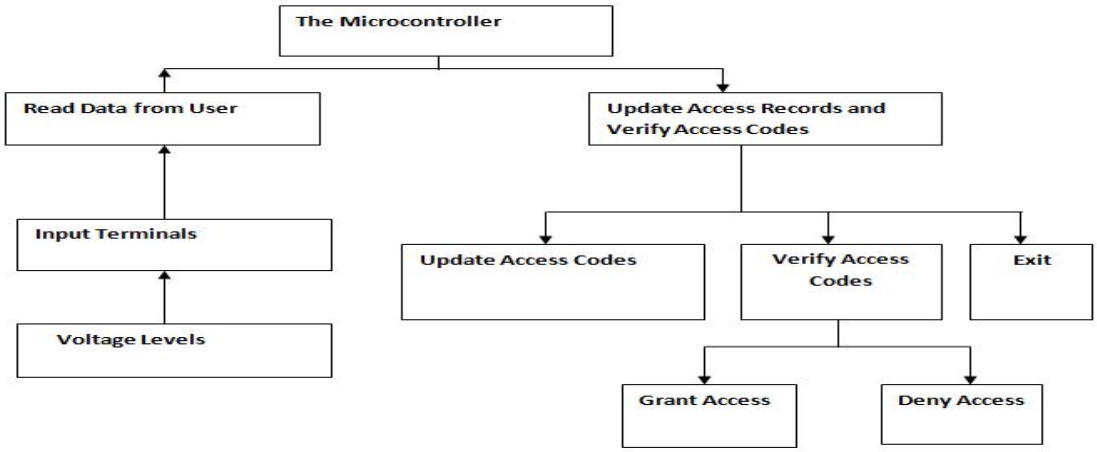

Fig. 3. High Level Model of the Proposed System

In the figure 3 above, the microcontroller at the apex of the model coordinates every other sub-section of the system. It runs an embedded application which helps it to manage its resources and communicate with other peripherals like screen and input terminals (keypad). The keypad monitors the changes at the voltage level of certain ports of the microcontroller (Port C) and generates the appropriate interrupts when the voltage levels changes. These interrupts

are captured by the microcontroller and read as input to the system. It generates different interrupt flags when the keypads are pressed. On generating the interrupts, the system picks the data and performs the specification required of it. There are different interrupts for increasing number, decreasing number, selecting number and accessing the screen. When the enter input terminal is selected, the system processes the selected codes and verifies the credibility of the user. The outcome of this verification results in the automation of the door mechanism of the system or house been locked. The drive system consist of a pair of bipolar transistors (NPN) as well DC motor.

B. Cost Evaluation of the Proposed System

Several software's and hardware components were needed for the design and implementation of the system. Table I shows the complete list of all the players in the team that led to the successful implementation of the system.

TABLE I. COMPONENTS COST ANALYSIS OF THE PROPOSED SYSTEM

S/N	Materials Used	Unit	Cost ($)
1	OshonSoft Integrated Development Suit	1	25
2	ISIS Professional Modelling and Simulation Software	1	30
3	Microcontroller Unit	1	15
4	Digital Multimeter	1	10
5	40-pin Socket	1	1
6	Soldering Lead	1 pack	6
7	LCD Digital Screen	1	3
8	Vero-board	1	1
9	12V Battery	1	15
10	7805 Regulator	1	1
11	1000 uf Capacitors	1	1
12	10uf Capacitors	1	1
13	1k Resistor	1	2
14	Crystal oscillator (12MHz)	10	11
15	Plastic Casing	1	5
16	Wooden Box	1	3
	Total		**135**

C. Advantages of the Proposed System

The proposed system would be very useful to the home, office or any other place where it is deployed because of the digitalization it brings to normal access control mechanisms

- The system is very intelligent and ensures proper security
- It ensures that the user doesn't have to worry about forgeting or misplacing physical keys.
- It enhances human experience of door lock system; the user doesn't need to have any form of physical contact with the door itself.
- It is very reliable and uses embedded technologies with a proven performance index.
- It's output is in digital form; this means that the system may be easily interfaced with other digital systems.
- It uses D.C power supply whose availability can be sufficiently guaranteed.
- The system allows the owner to reset the pass-code in event of someone accidentally seeing it.
- The proposed algorithm offers a great benefit where the user can change the PIN as many times as possible without the services of a programmer.

D. Disadvantages of the Proposed System

- The system due to its security check, didn't create room for password retrieval if forgotten.
- If someone inputs erroneous pass-codes more than a certain number of times, the system cannot captures and transmits an image of the person. It only stops the trial access of the person.

III. SYSTEM DEVELOPMENT METHODOLOGY

A system development methodology refers to the framework that is used to structure, plan, and control the process of developing an information system. A wide variety of such frameworks have evolved over the years, each with its own recognized strengths and weaknesses. One system development methodology is not necessarily suitable for use by all projects. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations. Common methodologies include waterfall, prototyping, iterative and incremental development, object oriented analysis and design methodology (OOADM), Spiral development, structured system analysis and design methodology (SSADM), rapid application development (RAD), extreme programming, joint application development methodology (JAD), and various types of agile methodology. Some people consider a life-cycle "model" a more general term for a category of methodologies and a software development "process" a more specific term to refer to a specific process chosen by a specific organization. For example, there are many specific software development processes that fit the spiral life-cycle model.

IV. SYSTEM DESIGN

A. Language Justification

Embedded Systems and embedded technology based intelligent systems and its derivatives may be implemented in a variety of languages depending on factors such as complexity, interoperability and convenience or technical skill of the programmer. These languages are C, C++, Embedded Pascal, Embedded Basic, assembly Language, etc. Naturally, the complexity of a work can narrow the work down to a particular programming language while the ability to run functions, procedures or threads written in another language may favor another language. Also, the technical strength and experience of the systems programmer cannot be over-emphasized.

Considering all these, Embedded Basic was chosen for the system's implementation due to the complexity of the work as well as a result of the developer's technical experience.

B. Input and Output Specifications

The input data to the system generated from the control terminals are decimal digits which are generated from humans pressing the buttons. The input is such that seven different buttons, INC, DEC, SEL, ENTER, CHANGE_PASSWORD and TYPE_PASSWORD. These buttons generate interrupts when pressed. The output consists of data and control information. The data is used to update the current state of the system while the control data is used to drive the security lock mechanism when necessary.

C. Program Flowchart

The flow chart used in modeling the entire system's functionality and behavior is shown below:

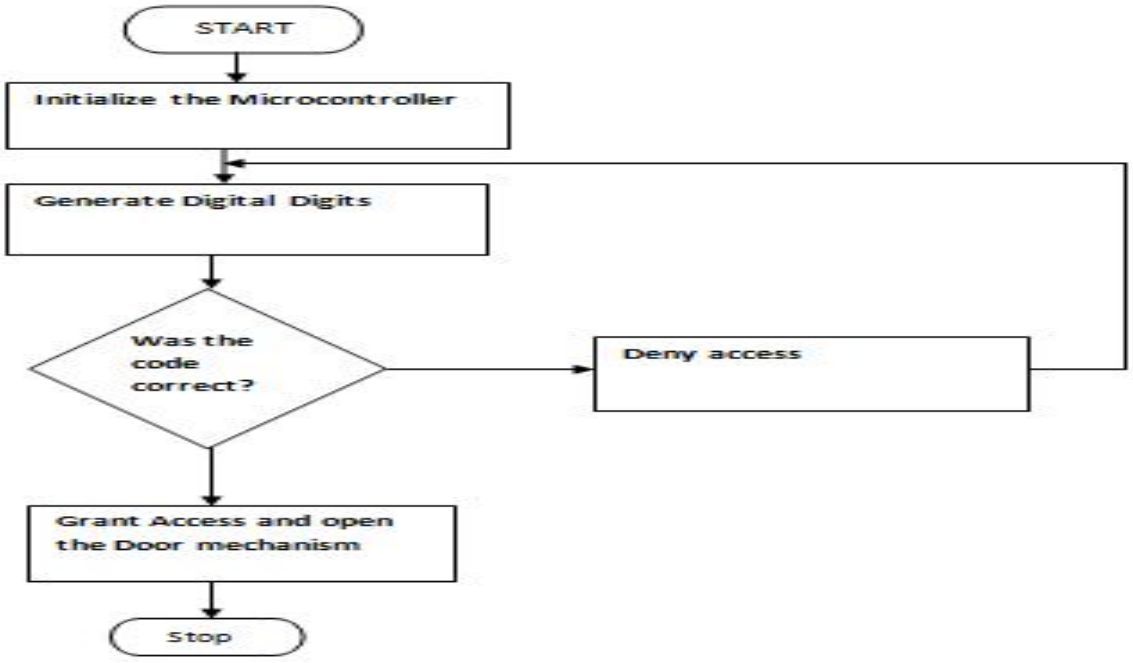

Fig. 4. Program Flowchart

1) Start: The procedure begins when the system is powered ON.

*2) Initialization of the microcontroller:*The system acquires input data from the user as a form of data collection. After which The enter botton is pressed to store this PIN. The input code is saved as a personal identification number (PIN).

3) Generate Digital Digits: the user is required to enter the same PIN for Re-identification procedure each time access is required by the user.

4) Correct Code: If the PIN entered by the user matches the PIN stored in the system, access is granted by the system.

5) Incorrect Code: If the PIN entered by the user does not match the PIN stored in the system, access is denied by the system.

6) Stop: the procedure is terminated when the following condition is met;

- The input code matches the PIN stored in the system
- Access granted and the lock opens

D. Program Algorithm

The detailed breakdown and simplification of the system's functional details are captured in the following algorithm:

10 Power ON the system
20 Initialization of the microcontroller
30 Acquire input data from the user
40 Was ENTER button pressed? If yes, READ the input digits, GOTO 50
Otherwise GOTO 30
50 Is the Input Code Correct? If yes, GRANT ACCESS to the USER, GOTO 30
Otherwise, GOTO 60
60 Is Input Code Incorrect? If yes, DENY ACCESS to the USER, GOTO 70
Otherwise, GOTO 60
70 STOP

V. System Requirement Specifications

A. Hardware Requirement Specifications

The hardware requirements of the system are specified as follows:

- The system must run on at least 8-bit microcontroller.
- The system must use ATMEGA series microcontrollers.
- The DC motor driving the box must have at least a torque of 1.5NM to be able to properly drive the mechanism.
- The input terminal must be metal switches (buttons) with plastic surface.
- The system must run on +9V or 12V DC power supply; though this may be adapted to include A.C power for redundancy. Redundancy becomes a necessity during the final deployment.

B. Software Requirement Specifications

The systems software requirement is as follows:

- An operating system of windows 7 or later versions, it can also run on LINUX OS.
- OshonSoft Integrated Development Suit for coding and part simulation of the system.
- ISIS 7 professional simulation software or later version for the complete simulation of the system
- The computer system running the software's must have at least 32 bit word length.

VI. Result and Discussion

The essence of this paper is to take a look at the various problem associated with the existing system which are viability to operate automatically, physical keys etc. with all these problems been critically analyzed a solution was embarked on to eliminate these problems with the design of an electronic safe. The system is powered ON to initialize the microcontroller. As a first time use, the system acquires input data from user and store it as a Personal Identification Number (PIN) on the system when the enter button is pressed. This process can be termed data collection and it is done once. Whenever the user seeks to be granted access by the system, the system requires that the user provides the same PIN that was initially stored on the system as a form of re-identification. Once the PIN is entered correctly, the lock opens and the user is granted access otherwise the user is denied access. The outcome of the request is displayed on the LCD as shown in figure 6. The result shows the flexibility and responsive reliability of the system. The cost for designing and implementing a unit of the electronic locking system is comparatively cheap compared to previous methods. This implies that manufacturers will save more cost considering industrial mass production of this device. It could be seen from the result that the system is more reliable to secure properties and data at a reduced cost.

VII. System Implementation and Testing

The system's implementation spans across several functions; from hardware Implementation to software programming and burning of the code into the target Chip.

A. Hardware Implementation

The circuit model is now carefully implemented using circuit board and soldering iron.
As shown below, the microcontroller, LCD, input terminals, relays, Transistors, regulators and resistors are mounted and interfaced on the Vero board. The completed circuit was troubleshooting to check for faults and certain unnecessary open and closed circuits.

B. Programming and Coding of the System

After the completion of the soldering, the development interface was run and used in the coding and simulation of the system. This is shown in figure7 below.

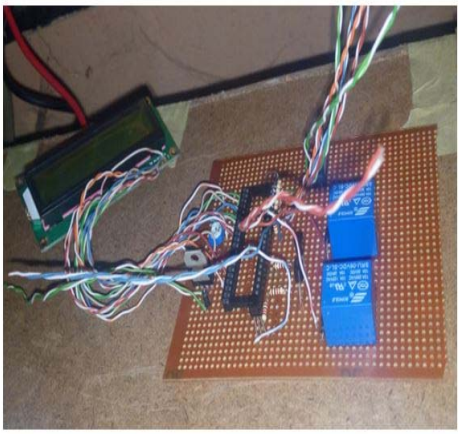

Fig. 5. System Implementation

Fig. 6. Complete keypad

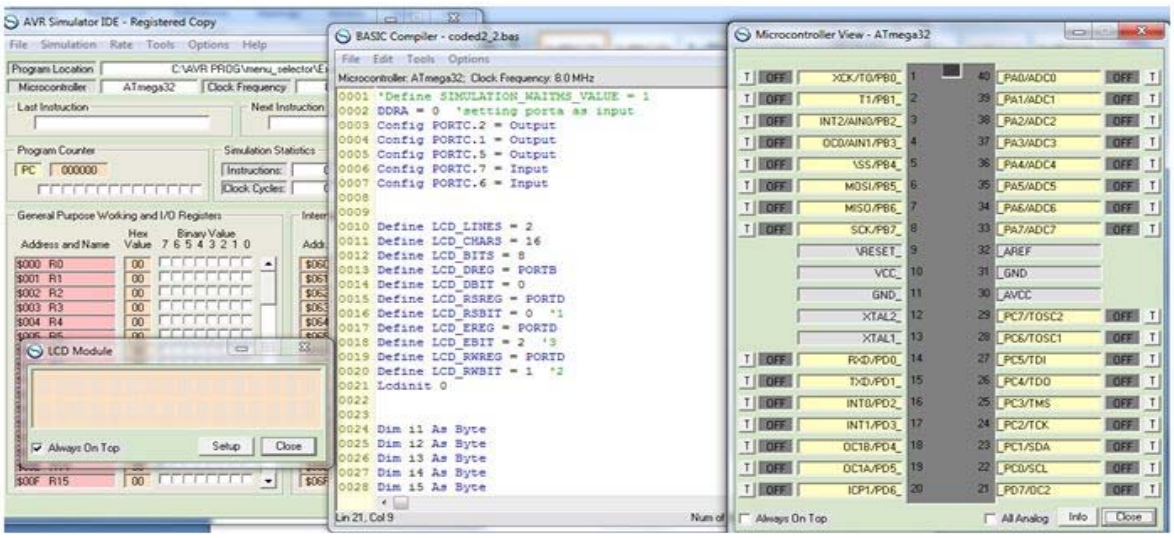

Fig. 7. OshonSoft Integrated Development Environment

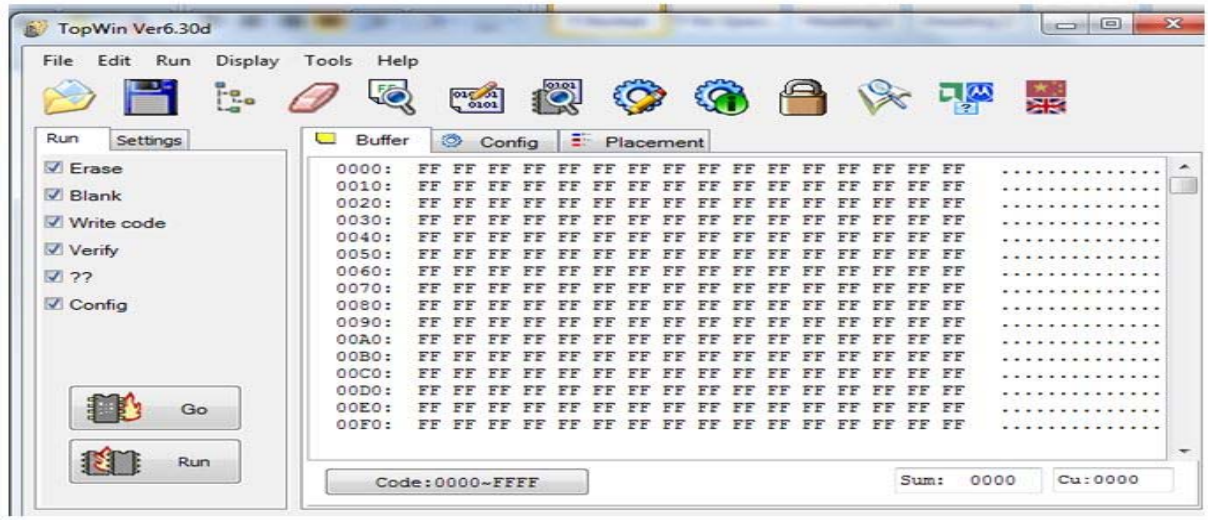

Fig. 8. TOPWIN Programmer Interface

After the compilation of the embedded code, a hex file was generated. The hex was transferred to the intelligent microcontroller through TOPWIN programmer software. The interface for the programming of the microcontroller is shown in Figure 8.

The following steps are followed in burning the "HEX FILE" into the program memory of the microcontroller:

- Plug the programmer to the computer and run the TOPWIN application program
- Select file menu and click Open; navigate the location of the program whose burning is sought and click OK.
- Click on Select Chip icon on the Menu Pane and navigate to the particular microcontroller or microprocessor of choice and click OK.
- Select Configuration and configure the frequency and clock of the target device
- Plug the microcontroller chip into the programmer's socket.
- Click Go and allow the system to display "Burning Completed" on the Screen.

VIII. Review of Achievement

This paper presents a model of an embedded technology to solve man's problems. It is also intended to portray the use of microcontrollers in processing/ controlling of data. It highlights the means of communicating with the microcontroller and the benefits of microcontroller. In real world, the application of this work can be modified to suit homes, offices and any application that requires a lock mechanism. Even in our regular automobiles.

IX. Conclusion and Future Work

The outcome of this paper shows the system flexibility, reliability, responsiveness and how it equally helps for security of properties and data. This paper seeks to encourage and arouse the interest of the general public on the availability and use of better method of security and shows how programming and digital electronics can be

effectively combined to enhance security. The proposed algorithm offers a great benefit where the user can change the PIN as many times as possible without the services of a programmer. However, the proposed algorithm has a limitation. It does not offer any option in a situation where the user forgets the PIN. Future work can be done to improve the proposed algorithm in order to offer better options in a case where the user forgets the PIN and also the system should be able captures and transmits an image of the person inputting erroneous pass-codes more than a certain number of times. Attributes such as finger print and face recognition could be integrated in this proposed algorithm which could help to retrieve forgotten user PIN. This will make the system security robust.

REFERENCES

[1] The August Smart Lock's not so 2-Factor Authentication (Part 1), February 2015, [online] Available: https://jmaxxz.com/blog/?p=476

[2] V. Sivaraman, A. Dhamdhere, H. Chen, et al., "An experimental study of wireless connectivity and routing in ad hoc sensor networks

[3] K.Y. Lian, S.J. Hsiao, W.T. Sung, "Mobile Monitoring and Embedded Control System for Factory Environment," Seneor, vol. 13, no. 12, pp. 17379-17413, December 2013.

[4] P.P. Gaikwad, J.P. Gabhane, S.S. Golait, "A survey based on Smart Homes system using Internet-of-Things,"Computation of Power, Energy Information and Commuincation (ICCPEIC), pp. 330-335, April 2015.

[5] Chi-Huang Hung, Ying-Wen Bai, Je-Hong Ren Design and implementation of a single button operation for a door lockcontrol system based on a near field communication of a smartphone 2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCEBerlin) J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[6] Sayidul Morsalin, A. M. Jahirul Islam, Golam R. Rahat, Syed R. H. Pidim, Abdur Rahman, Md A. B. Siddiqe Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application 2016 3rd International International Conference on Trends in Electronics and Informatics ICEI 2017 978-1-5090-4257-9/17/$31.00 ©2017 IEEE 715 Conference on Electrical Engineering and Information Communication Technology (ICEEICT)

[7] W.T. Sung and C.C. Hsu, "IOT System Environmental Monitoring using IPSO Weight Factor Estimation", Sensor Review, vol.33, no.3, pp.246-256, July 2013.

[8] K. Mukherjee and D. Chatterjee, "Augmentative and Alternative Communication Device Based on Eye-Blink Detection and Coversion to Morse-Code to Aid Paralyzed Individuals," Communication, Information & Computing Technology(ICCICT), pp.1-5, January 2015.

[9] L.R. Sapaico and M. Sato, "Analysis of Vision-based Text Entryusing Morse Code generated by Tongue Gestures," Human System Interactions (HSI), pp.158-164, May 2011.

[10] N.P. Kumar and R.K. Jatoth, "Development of Cloud Based Light Intensity Monitoring System Using Raspberry Pi," Industrial Instrumentation and Control (ICIC), pp.1356-1361, May 2015.

[11] D. Naresh, B. Chakradhar, "Bluetooth Based Home Automation and Security System Using ARM9", *International Journal of Engineering Trends and Technology (IJETT)*, vol. 4, no. 9, Sep 2013

[12] Jiakailin Wang, Jinjin Zheng, Shiwu Zhang, Jijun He, Xiao Liang, Sui Feng A Face Recognition System Based on Local Binary Patterns and Support Vector Machine for Home Security Service Robot 2016 9th International Symposium on Computational Intelligence and Design (ISCID)

[13] Md. Nasimuzzaman Chowdhury, Md. Shiblee Nooman, Access Control of Door and Home Security by Raspberry Pi Through Internet International Journal of Scientific & Engineering Research, vol. 4, no. 1rjober-2013.

[14] Subhajit Dey, T Kundu, "Web Based Real-Time Home Automation and security system", *IJEETC*, vol. 4, no. 3, July 2015.

[15] Zhaoqing Peng, Takumi Kato, Hideyuki Takahashi, Tetsuo Kinoshita Intelligent home security system using agent-based IoT devices 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE).

[16] A. Daramas, S. Pattarakitsophon, K. Eiumtrakul, T. Tantidham, N. Tamkittikhun HIVE: Home Automation System for Intrusion Detection 2016 Fifth ICT International Student Project Conference (ICT-ISPC).

[17] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose, Lakshmi Boppana IoT based smart security and home automation system 2016 International Conference on Computing, Communication and Automation (ICCCA)

[18] F. L. Zucatto, C.A. Biscassi, F. Monsignore, F. Fidelix, S. Coutinho, and M. L. Rocha, "ZigBee for Building Control Wireless Sensor Networks," in proceeding of Microwave and Optoelectronics Conference, pp. 511- 515, Oct. 2007.

[19] Il-Kyu Hwang and Jin-Wook Baek, "Wireless Access Monitoring and Control System based on Digital Door Lock," IEEE Trans. On Consumer Electronics, Vol. 53, No. 4, Nov. 2007. pp 1724-1730.

[20] A. Wheeler, "Commercial Applications of Wireless Sensor Network Using ZigBee", IEEE Communications Magazine, V. 45, N. 4, pp.:70 – 77, April 2007.

[21] Kasim Adalan, Burcu Erkmen Face recognition, NFC and voice controlled door lock system 2016 National Conference on Electrical, Electronics and Biomedical Engineering (ELECO)K. Elissa, "Title of paper if known," unpublished.

[22] Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit Design and implementation of a fingerprint based lock system for shared access 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).

[23] Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982]

[24] Ashwini Ashok Mandavkar, Rohini Vijay Agawane Mobile based facial recognition using OTP verification for voting system 2015 IEEE International Advance Computing Conference (IACC)

[25] S. Chitnis, N. Deshpande, and A. Shaligram, "An Investigation Study for Smart Home Security: Issuse, Challenges and Countermeasures," Wireless Sensor Network, vol. 8, no. 2, pp. 61-68, April 2016.

[26] ZHANG Ping, "'Open, sesame' Design of intelligent lock," Journal of Hebei University of Technology, April 2015.

[27] A. Bianchi, I. Oakley, H. Kim, "PassBYOP: Bring Your Own Picture for Securing Graphical passwords," Transactions on Human-Machine Systems, pp. 1-10, 2015. [25] D. Florencio and S. Herley, "a large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web, pp. 657-666, 2007.

[28] K. Solanki and P. Pittalia, "Review of Face Recognition Techniques," International Journal of Computer Applications, Vo. 133, no 12, pp. 20- 24, January 2016.

View publication stats