Design of a Programmed AT89C52 Microcontroller Access Door Control System

Chukwudi Emeka Udu, Chika Edith Mgbemena, Okechukwu Chiedu Ezeanyim, and Charles Chikwendu Okpala*

Department of Industrial/Production Engineering, Nnamdi Azikiwe University, P.M.B. 5025 Awka, Anambra State, Nigeria

**Correspondence Address*

Abstract: **Biometric systems installed on doors cannot be used by everyone, as it is unhealthy for someone to touch a device that has already been pressed by so many others. Also, people without hands cannot use fingerprint or hand-based systems, while visually impaired people have difficulties using iris or retina based techniques. To overcome these challenges, a programmed AT89C52 microcontroller access door control system that makes use of two multi-factor user authentication with password and smartcard was designed to restrict the entry of unauthorized persons from sensitive or highly secured areas. Unified Modeling Language was used to model the functionality of the system with AT89C52 microcontroller, power supply, keypad, display unit, smartcard, smartcard reader, relay driver and dc motor as hardware. The card reader was designed with a Random Access Memory card reader slot in a computer's central processing unit connected to the port 0 of the AT89C52 microcontroller. While the software program used for the programmable AT89C52 access door control system was successfully programmed with assembly language in order to perform the desired assignment, the source code was developed in an integrated development environment. The entire software which was arranged by integrating all the modules in a main control loop, and tested for conformity with the main control program alongside the hardware, achieved its objective of deterring unauthorized attempt to highly restricted areas.**

Keywords**: AT89C52 microcontroller, security, access control, software, hardware, code, password, random access memory, authentication**

I. INTRODUCTION

Access control system is a great accomplishment that keeps rewarding the world with security of lives and property. It is a system that allows access to authorized users, and also denies access to unauthorized persons. The need for a robust access control cannot be over-emphasized as the installation of key lock on doors has no restriction when entrance key falls into the hands of an unauthorized user.

A door is a relatively solid but movable surface, opaque, wholly or partly glazed, usually of wood, metal, glass, or a combination of materials, that closes an entrance to a building or a room, and is fixed in an opening in a wall whose purpose is to act as barrier and also prevent unauthorized entrance. Doors can also be used to screen off areas of a building for aesthetics and other purposes, and are also generally used to separate interior spaces like rooms, closets, etc. for privacy, convenience, security, and other reasons.

Chomo, Yawas, and Johnson (2018), pointed out that automatic door system was started and popularized by the supermarkets in the United States of America, as a result of the search to ameliorate the hardship experienced by shoppers. However, an automatic door control system give access to both authorized and unauthorized persons, as its inability to perform authentication was its major security flaw.

A smart card is a plastic card about the size of a credit card with an embedded micro-processor chip mainly used for authentication and authorization. This simple technology has been revolutionized and thereby increases the level of card security. Today, smart card technology is the efficient path to the future, and find its application in different walks of life such as in the banking sector where microchip is used to authenticate processes that protect users and bank from fraudulent activities. In health care, extensive health data of an individual can be stored in small chips that in turn can relay information to insurance companies or medical professionals.

In E-passport, it allows for the storage of digital version of the identity card photo and data that is found on the first page of the paper passport. In information technology, it secures authentication and user login, amplifier encryption of sensitive data, credentials, digital certificates etc. Also, in mobile technology, smart card secures mobile value-added services, as well as subscriber's authentication. While in electronic purse, smart card stores monetary value for small purchases where the card reader retrieves the amount that is stored in it, and subtracts the amount being used for purchasing of goods.

II. LITERATURE REVIEW

Okner (2021), explained that a typical contact setup for access control is an access controller which takes decision, manages lock and unlock schedule and performs many other activities related to authentication and authorization at the point of entry. This design is an access control system based on multi-factor user authentication, a combination of possession based and knowledge based authentication that acts as a security watchman that ask a question like "who are you?"

According to Lal et al. (2016), the correct answer to the question is the proof of identity which only the authorized user can provide. However, the access controller is the brain-box of the system designed with AT89C52 which has the ability to check information provided at the entry terminal using assembly language to write the program into the microcontroller. It performs authorization through its binary YES or NO decision to arrive at an answer if the user should be granted or denied access. The validation of a user's identity uses two variables of something one has (the user inserts a smart card) and something one knows (the user inputs password) to gain access.

Khan, and Dristy (2015), designed android based security and home automation system using a PIC microcontroller to maintain security in the home's main entrance, and to control car door lock and other appliances in a house.

Amunullah, (2013), designed a microcontroller based reprogrammable digital door lock security system using matrix keypad and the Global System of Mobile/Communication Code Division Multiple Access (GSM/CDMA) network. When a valid code is entered through the matrix keypad the door opens. Similarly when a phone call is made from the desired number, the GSM/CDMA module in the system unlocks the door. Its Instant Power Supply (IPS) circuit gives feedback when there is a power failure. The system uses a desired mobile number without verification and does not have a true sense of mobility. Therefore, there is a need for true remote and adequate secure solution that should be effective and also realizable.

Ajay, Shelja, and Swati (2014), designed and developed a sensor based home automation security system with the application of a GSM module and locking system to detect an intruder using diffused In-line Infrared (IR) sensor. Here the shock sensor locks the intruder out of the door, while the GSM module sends a short message service (SMS) as an intruder warning alert to the people inside.

Jain et al. (2016), designed a password protected home automation system with an automatic door lock. In the system, an Arduino Uno microcontroller board is used for interfacing the various hardware peripherals. The door, light and fan are controlled when the valid password matches the pre-decided password in the microcontroller.

Akubue (2016), designed a door control with the application of a smart card and interactive code lock. The microcontroller (AT89C51) was programmed with visual basic, which is capable of reading inserted smartcard and authenticating passwords. In the system, the door automatically closes after 30 seconds irrespective of any entrance or not. However, there is a need for more waiting time before the deactivation of the keypad and screen display.

Lee et al (2017), designed and implemented enhanced smartcard-based password authenticated key using extended chaotic maps that have the capacity of withstanding vulnerability to denial-of-service attacks and privileged insider attacks.

Gupta et al. (2019), proposed the implementation of a smartcard for a vehicular information system that is intended to store all vehicle related crucial information such as the vehicle's Registration Certificate (RC), vehicle owner's Driver's License (DL) for five users in a family, vehicle's insurance, pollution details, and vehicle owner's details unto one single card. This will eliminate the need for multiple cards and documents that the vehicle owner needs to carry about and each vehicle owner's card would be identified with a unique serial number to support the government's smart city vision.

Mcs-51 Assembly programming

According to Visa and Asogwa (2012), the Intel AT89C52 microcontroller is a complete computer on a single chip. The first 8-bit microcontroller was produced by Intel in 1976, and its improved version of 16-bit was released in 1982. In the world view of microcontroller, programming is a written sequence of instructions that are executed by the processor in a particular order to perform a predefined task. It involves debugging, troubleshooting and sequencing of instruction to ensure the desired task is performed. According to Keil (1995), programming languages have specific words, grammar and rules guiding them. Based on these guidelines and relationship, microcontroller has three levels of programming which include: machine language, assembly language, and high level language.

Alu (2021), pointed out that machine language code is written in binary bit patterns such as the combination of binary digits 1 and 0, which are stored as high and low voltage levels. This language is the lowest level of programming language that the microcontroller understands.

Assembly Language is a Pseudo-English representation of the Machine Language. It is a combination of English-like words called Mnemonics and Hexadecimal codes. An assembly language program is a written computer program (mnemonics) that can be translated directly into a machine recognizable form that is capable of instructing the microprocessor what operations to perform. This translation is performed with a software tool known as an assembler. It is designed to simply perform clerical task of translating written computer programs to executable codes.

Assembly language is a low level language that requires an extensive understanding of the architecture of microcontroller. While assembler is a program designed to convert programs written in assembly languages to machine code. The ASEM-51 assembly language is a rich subset of the Intel standard that

guarantees maximum compatibility with existing assembler sources to implement all 8051 instruction mnemonics, useful subset of the Intel pseudo instructions and assembler controls. It is also suitable for small and medium MCS-51 based microcontroller projects.

The high-level language use words and statements that are easily understood by humans and do not require the architecture or other internal details of a microcontroller. A compiler is a program designed to convert written high-level languages to machine code. Examples of high-level languages are BASIC language, C-Pascal language, C++ language and Java language. The advantages assembly language programming has over high-level programming are the ability to execute instruction faster and to occupy less space. Its assembler is reliable, compact and well documented. The advantages and features that make assembly language the preferred choice include: generation of Intel–Hex file output easily, bootstrap program for testing on the MCS-51 target board, automatic code optimization of generic jumps and calls, as well as the availability of its assembler.

III. METHODOLOGY

System Modeling

System modeling is the use of models to conceptualize, construct and show how processes interact in a functional system. The use case diagram as shown in figure 1, which is a dynamic or behavior diagram in Unified Modeling Language (UML) was used to model the functionality of the system. The system is usually developed, designed or operated, while the actors are people or entities who operate under defined roles within the system. In this study, the system is the access door control, while the actors are the card holder and system programmer.

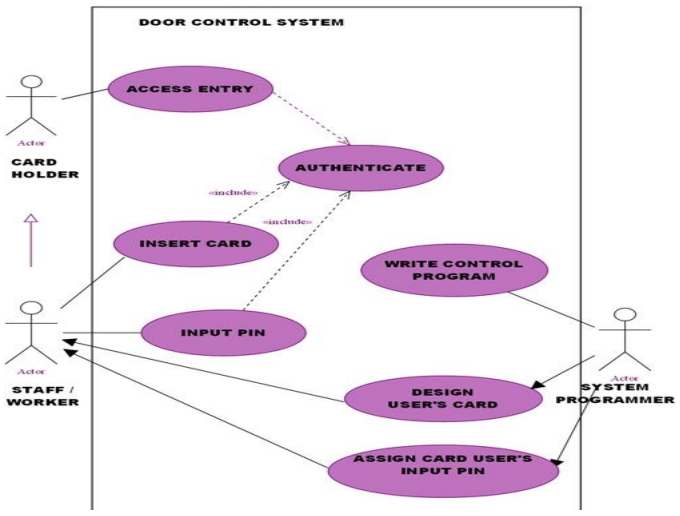

Figure 1: Use case diagram

Activity diagram of the system

An activity diagram is a very important diagram in unified modeling language used to describe the dynamic aspects of the system. It represents the flow from one activity to another activity. The activity diagram is used to describe the operations carried out in the system from start to stop as shown in Figure 2.

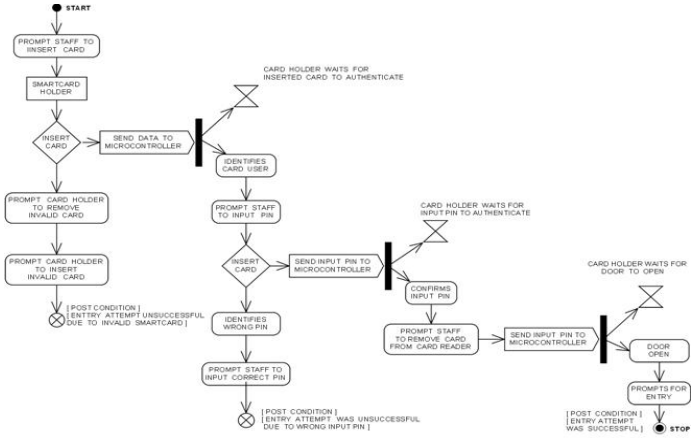

Figure 2: Activity diagram

Hardware Design

The hardware is comprised of an AT89C52 microcontroller, power supply, keypad, display unit, smartcard, smartcard reader, relay driver and dc motor as depicted in Figure 3.

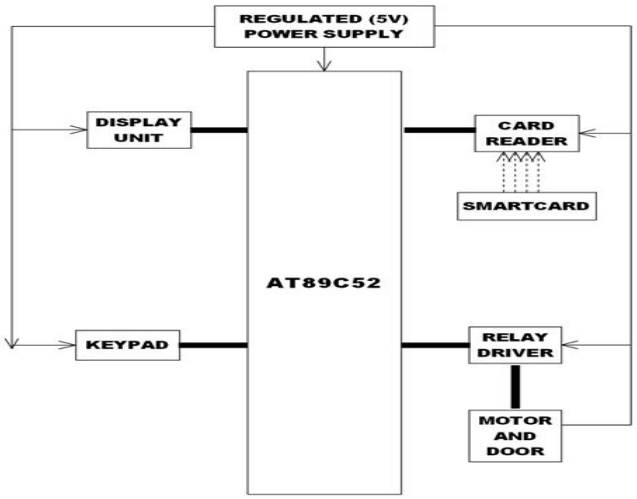

Figure 3: Block diagram of the system

Smartcard Design

Contact smartcard interface is extended in the design, and is designed with 555 timer soldered on a rectangular piece of vero-board to serve as the card chip. The 555 timer is configured as a one-shot mono-stable multi-vibrator to provide a high state through its output trigger (pin 3) as shown in Figure 4.,

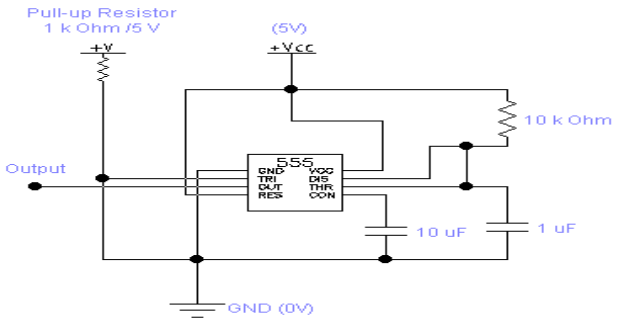

Figure 4: Mono-stable Multi-vibrator

Once energized, the 555 mono-stable will remain in this high output state until it is removed from the card reader.

The output pin can drive any TTL circuit and is capable of sourcing or sinking up to 200mA of current at an output voltage equal to approximately 1.5V, and this value is more than enough to drive or switch other logic ICs, LEDs or small lamps. With this specification, it is convenient enough to connect the microcontroller directly to the output. The high state or logic "1" serves as data that is transmitted through the card reader to the microcontroller. The 555 timer on the card is energized through the PIN 8 (VCC) and PIN 1 (GND) when the smartcard is inserted into the card reader.

Smartcard Reader Design

The card reader is designed with Random Access Memory (RAM) card reader slot in the computer (CPU) connected to port 0 of the AT89C52 microcontroller. The card reader slot is capable of containing the thickness of the vero-board. The pinouts are connected to the port 0 of the microcontroller. When the smartcard is inserted into the reader, the high state from output pin 3 is transmitted through the card reader to port 0 of the microcontroller for authentication. The data transmitted into the port 0 is used to identify the card user. It is also used for instructing the next operation to be performed as it is programmed into the microcontroller.

AT89C52 Microcontroller

The microcontroller used is AT89C52. It is a low power, high performance CMOS 8-bit microcontroller with 8Kilobytes of Flash Erasable and Programmable Read Only Memory (EPROM). The device is manufactured using Atmel's high density non-volatile memory technology. The on-chip flash allows the program memory to be reprogrammed in the system or by a conventional non-volatile memory programmer. By combining a versatile 8-bit CPU with flash on a monolithic chip, the Atmel AT89C52 as shown in Figure 5 is a powerful microcomputer that provides a highly flexible and cost-effective solution to many embedded control applications.

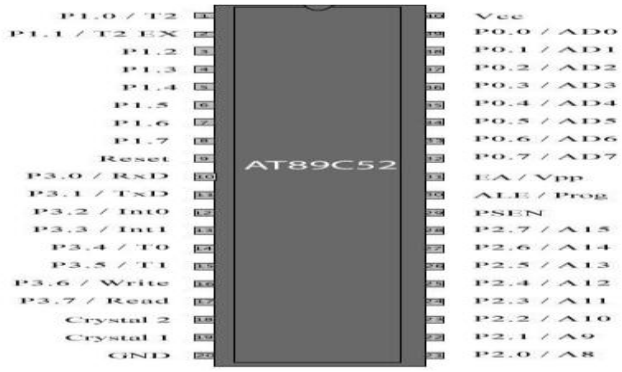

Figure 5: Atmel AT89C52

The AT89C52 provides the following standard features: 8k byte flash, 256 bytes of RAM, 32 I/O lines, three 16-bit timer/counter, six-vector two-level interrupt architecture, a full-duplex serial port, on-chip oscillator, and clock circuitry.

Matrix Keypad

A matrix keypad consists of an arrangement of push buttons in matrix format in rows and columns with the microcontroller I/O pins connected to the rows and columns of the matrix such that push buttons in each row are connected to one pin of the microcontroller and the push buttons in each column are connected to another pin of the microcontroller. In this design, a 3x4 matrix keypad is used as shown in Figure 6.

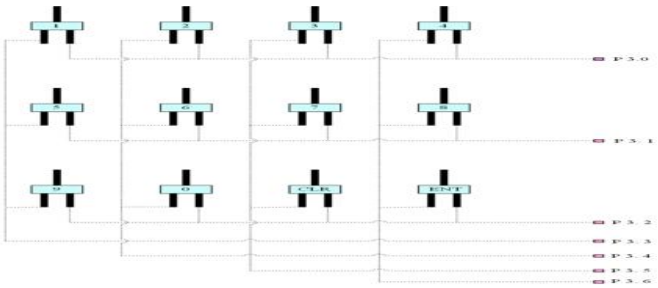

Figure 6: Matrix keypad

Display unit

The display screen is comprised of six (6) LED display of common anode arranged in serial port mode. A seven-segment display is one of the efficient types of display used in an electronic display device for decimal numbers from 0 to 9, alphabets and basic characters in electronic devices like microwave ovens, calculators, washing machines, radios, microcontroller projects and digital-clocks. Seven segment have eight (8) LED separated into segments which can be named a, b, c, d, e, f, g, Dp pin pulled out of the module and the other pins pulled out as the common pin. Common anode as depicted in Figure 7 is the type of seven segment used in the design.

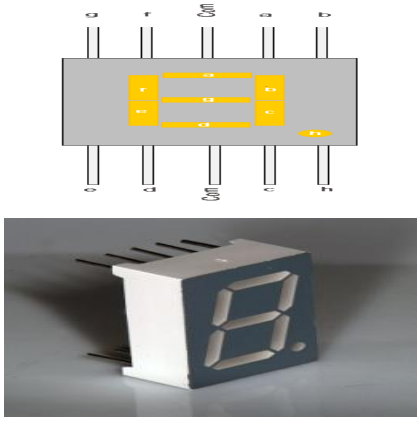

Figure 7: Common anode seven segment

Working principles of the system

The power supply circuit of the hardware design is connected to a 230v AC power source. The regulated (5v) power supply is used to energize the AT89C52 microcontroller, the keypad, relay driver and the display unit of the system. The display unit prompts the card holder to insert a card into the reader for authentication. Through the written program, the microcontroller begins to scan the smartcard reader through port 0. When the card is inserted, it makes physical contact with 5v that energized a mono-stable circuit embedded in it.

The stable high output logic '1' sets the bit in port 0 of the microcontroller. Through the written program, the microcontroller identifies the card user and prompts the card holder to enter a secret pin for authentication. The microcontroller sends #0FFH to port 3 before scanning the push buttons in the keypad. When push button 1 is pressed, it clears logic 1 in P3.0 and P3.3 to logic 0. From the written program, the microcontroller sends data #1 (decimal number 1) to the display unit. This operation is applicable to numbers from 0 to 9.

After the four-digit pin is entered into the display unit, the card holder is prompted to press the enter button. The enter button clears logic 1 in P3.2 and P3.6 to logic 0. When these two bits are made logic 0, the microcontroller authenticates by comparing the four secret data in the display with the data written into the microcontroller. If they are different, the microcontroller sends data to the display unit indicating ACCESS DENIED. If the four secret data are confirmed to be the same, the microcontroller sends data to the display unit indicating PLEASE ENTER.

The microcontroller makes the logic level of P2.6 to be "1" and the logic level of P2.7 to be "0". Through the P2.6 and P2.7 of the microcontroller, the two terminals of the motor driver are connected to positive (+ve) and negative (-ve) terminals of the 12V DC motor, and controlled with the help of written program to turn clockwise and anti-clockwise. These directions represent the opening and closing of the door.

System Implementation

The various sections of the hardware systems and software systems are implemented using different circuitry formulations that satisfy the aim of the design and software coding using assembly language that provides appropriate control as specified.

IV. DISCUSSION OF RESULTS

The implementation of the hardware sub-system was achieved unit by unit. The input sub-system is a 4x3 matrix keypad as seen in Figure 6 to enable data entry and operation of the system. The matrix keypad designed and used in this project is shown in figure 8.

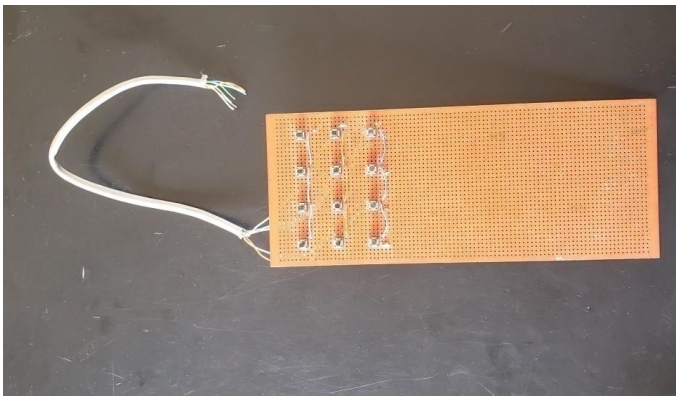

Figure 8: The 4x3 matrix keypad

To achieve a positive result, the AT89C52 microcontroller was connected directly to the keypad to access input using software coding to encode and decode a button press. The three-row terminals of the keypad are connected to P3.0 - P3.2 of the microcontroller while the four-column terminals of the keypad are connected to P3.3 - P3.6 of the microcontroller.

With the aid of the software tool, the separate parts of the sub-system were properly connected and simulated before carrying out the physical construction. To facilitate and reduce circuitry errors, the final circuitry was exported to another Computer Aided Design (CAD) software tool known as **Proteus ARES** which guides the production of all the lines linking one pin to another as shown in Figure 9. The CAD tool makes it possible to easily layout the various components on the board, and to define the position of each component before they are linked to one another by the traces.

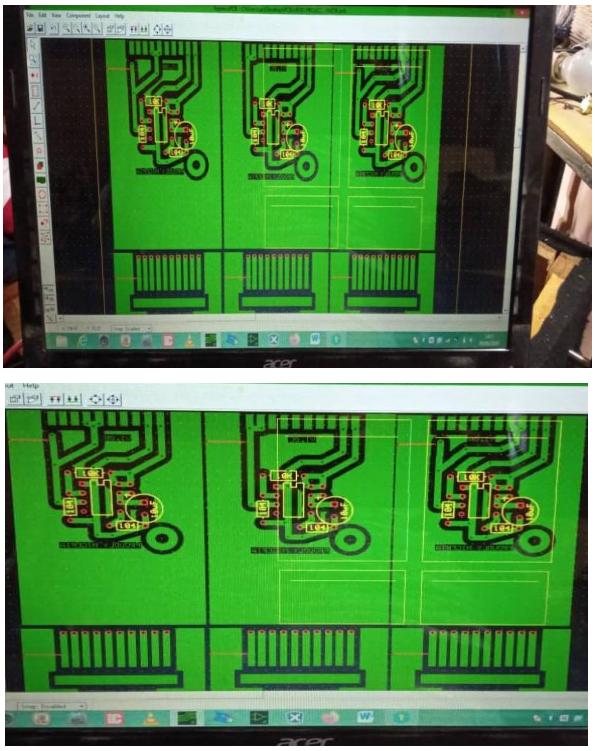

Figure 9: CAD software tool laying out the various components on the board

A mesh of the printed PCB layout size was formed by stretching it within a wooden frame as shown in figure 10. By the method of direct stenciling, an emulsion sensitized with a solution of ammonium dichromate which made the emulsion respond to ultraviolet (UV) light when exposed to the light was applied to the mesh. Once the mesh was coated, the emulsion was then dried on a heater and shaded away from light in a dark room to produce a screen. The screen was then exposed to ultraviolet (UV) light for about 20-35 seconds with the printed PCB film held tightly to the screen to produce a stencil.

This process transfers the PCB layout on the screen producing a negative stencil on the PCB print-out which is used to print the PCB layout on the copper clad board with ink. The copper-clad is firstly cleansed with a smooth sandpaper to remove any copper oxide deposited on the board.

Figure 10: A mesh of the printed PCB layout

The software program used for the programmable AT89C52 access door control system was written with assembly language. The source code was developed in an Integrated Development Environment (IDE), the general syntax of assembler statements, the assembler instructions and several assembler controls that influence assembler process and hex file generation were implemented using ASEM-51.

V. CONCLUSION

The successful design of the programmed AT89C52 microcontroller access door control system using two multi-factor user authentication methods is quite capable of providing a high level of security to hospitals, industries, banks and other organizations that are faced with the security challenge of restriction of unauthorized entry attempt to sensitive or highly secured areas.

In a highly competitive scenario, the design will be among the best proactive control systems that can deter unauthorized attempts to highly restricted areas. The ability to overcome challenges of finger touch which leads to vulnerability to virus attack, and the keeping of records that shows when card users enter or leave through a door, will make the design to be widely accepted in banks, hospitals, companies, as well as other organizations where access control is required.

REFERENCES

[1] Ajay, M., Shelja, D., and Swati, S. (2014). "Designed and Development of a Sensor Based Home Automation Security System with the Application of GSM Module and Locking System" International Journal of Advanced Engineering Research and Science, vol. 1, iss. 4

[2] Alu, A. (2021). "Binary Numbers" [Online]. Accessed on 18 January 2022, from https://www.electronics-tutorials.ws/binary/bin_1.html

[3] Akubue, T. (2016). "Door Controller Using Smart Card and Interactive Code Lock" International Journal of Advanced Research in Computer Engineering and Technology, vol 5, iss. 2

[4] Amunullah, M. (2013). "Microcontroller Based Reprogrammable Digital Door Lock Security System by Using Keypad and GSM/CDMA Technology" Journal of Electrical and Electronics Engineering, vol. 4, iss. 6

[5] Chomo, D., Yawas, D., and Johnson, Z. (2018). "Development of an Automatic Door System" American Journal of Engineering Research, vol. 7, iss. 5

[6] Gupta, K., Kumar, S. and Tripathy, M. (2019), "Implementation of Smart Card for Vehicular Information" International Journal of Engineering and Advanced Technology, vol. 8, iss. 5

[7] Jain, A., Shukla, A. and Rajan, R. (2016). "Password Protected Home Automation System with Automatic Door Lock" MIT International Journal of Electrical and Instrumentation Engineering, vol. 6, iss. 1

[8] Khan, S. and Dristy, F. (2015). "Android Based Security and Home Automation System" International Journal of Ambient Systems and Applications, vol. 3, iss. 1

[9] Keil Elektronik GmbH Inc., (1995). "A51 Assembler and A251 Assembler, Macro assemblers for the 8051and Mcs 251 microcontrollers" [Online]. Accessed on 22 January 2022, from https://www.scribd.com/document/150092010/A251

[10] Lal, N., Prasad, S. and Farik, M. (2016). A Review of Authentication Methods. "International Journal of Scientific and Technology Research, vol. 5, iss. 11

[11] Lee, T., Hsiao, C., Hwang, S. and Lin, T. (2017). "Enhanced Smartcard-Based Password Authenticated Key Agreement Using Extended Chaotic Maps" PLOS ONE, vol. 12, iss. 7

[12] Okner, D. (2021), "Understanding Access Control Systems" [Online]. Accessed from https://www.getkisi.com/access-control on 8 February 2022

[13] Visa, I. and Asogwa, V. (2012). "Microcontroller Based Anti-theft Security System Using GSM Networks with Text Message as Feedback" International Journal of Engineering Research and Development, vol. 2, iss. 10