Security Enhancement for Building Access, Using One Time Password (OTP) Technology

Uko Victor Sorochi, Nasiru Abdulsalam, and Isa Abdulrauf Inusa

Abstract—Ubiquitous as mobile technologies are, and the various advancements the technologies have experienced, makes the field pertinent for integration into security systems of buildings. As a security enhancement technique for building access, this project was proposed as a way of paving a way for integration of one time password (OTP) technology using microcontroller to security systems. In addition, the proposed project will be a supplement to the challenges of other security authentication methods centered on Bluetooth, radio frequency identification (RFID), biometrics and voice recognition techniques. In other to reduce complexity in design, a microcontroller was introduced to hub the coordination of the system. The two way verification system which can be coupled with aforementioned security systems, boast of its ability to store numeric identity of each authorized user to a building in the electrical erasable programmable read only memory (EEPROM) of the microcontroller. The system prompt a user wanting to gain access to the building through the door to input designated numeric identity (password) stored in data base. Once the inputted designated numeric identity entered matches an identity in the data base, then, for the second verification process, a randomly generated OTP which has a programmed validity of three minutes is sent to the user phone via a GSM (global system for mobile communication) module. If either the password or OTP entered doesn’t match, then access is denied and the user will only be relegated to two successful trials with time duration as programmed for retrieval, before the system reset for the next user. Once there is failure at any stage of verification outside prescribed attempted limit, an alarm is sounded with implication that a burglar is attempting entry. Electric power to the project was driven from an ac mains which was then rectified to power all the dc dependent components used. The low construction cost, user friendliness, flexibility, insured security when compared to other security systems, makes the innovation unique.

Index Terms—Authentication, building security, GSM technology, microcontroller and OTP technology

I. INTRODUCTION

Ever since man started making progressions in the construction of shelter over his head, security issues have always been a thing of concern for his safety. Various control systems have been designed over the years to prevent access to unauthorized users. The main aim for providing locks for our home, school, office and building is for security of our lives and properties. It is therefore important to have a convenient way of achieving this goal [5].

As an indication to man’s progressive efforts in securing buildings, mechanical lock systems were invented as a building panacea to bridge security gaps. Though the mechanical lock system served purpose, it was often prone to burglar attack by criminals. Furthermore, users of such mechanical locks umpteen times misplace keys to the lock system, leaving them with the only alternative of damaging the lock to gain access.

Direct human involvement in the operation of mechanical lock systems reduced the efficiency of the system and made the utilization of the system burdensome. To annul challenges of mechanical lock systems in rendering building security, automated systems evolved. Among the automated innovation grafted for granting access to buildings include: Bluetooth, biometrics, RFID (radio frequency identity) and voice recognition technologies.

The innovative architecture was not void of peculiar challenges. For example, the Bluetooth system has a limited range for operation. The biometric system is not private to users and can be easily hacked. The voice recognition system can be easily intercepted by recording users’ voice using playback audio recorders, while the RFID system suffers from cloning and spoofing.

As a security enhancement strategy, an automated system called a one time password (OTP) technology can be incorporated in any of the aforementioned building security system. The OTP technology can also act as a standalone security technology for building access and other multiple purposes as a security measure.

OTP is a string of characters or numbers automatically generated to be used for single login attempt. OTP can be sent to the user’s phone via SMS (short message Service) or push messaging and is used to protect web-based service, private credentials and data. OTP’s minimizes the risk of fraudulent login attempt and thus the risk of stolen data. OTP’s come in all shapes and sizes but always add an extra layer of authentication. [9]

The authentication system when used for building security access will practically be impossible for unauthorized users to gain access if well incorporated with aforementioned security methods or acting as a standalone. OTPs are not vulnerable to reply attack and have a great advantage on static password. [10]
A. Objectives of Study

- To establish a medium for enhancing building security based on OTP technology, which will either serve as a substratum for synergy with other building security techniques or as a stand alone development.
- To use microcontroller to reduce complexity of building security architectures.
- To develop software instructions for programming the microcontroller using the Arduino IDE (integrated development environment)
- To utilize GSM technology for security authentication.

B. Structure of the Paper

Section one in this paper, is an introduction that leads the reader from a general area of knowledge to the particular topic of investigation, as well as establishing objectives of the research.

Section two pillars the literature survey which reviews researches made by predecessors on similar subject of inquiry. The shortcomings from surveyed literatures will be bases for improvement.

The hub of the research methodology rest on the shoulders of section three. In this section, elaboration was made on mathematical designs, hardware and software approaches as well as criterial for selection of essential component used for the final implementation.

Section four gives account of results obtained from test made using the innovation. Lastly, section five expresses conclusions drawn from the study.

II. LITERATURE SURVEY

To curb the menace of insecurity with rising population, technological advances have been made on lock systems ranging from mechanical, analog and digital intervention schemes or any mesh of the listed methods. Invention of the combination lock set the stage for improvement of lock systems.

A combination lock is a type of locking device in which a sequence of symbols, usually numbers, is used to open the lock. The sequence may be entered using single rotating dial which interact with several discs or cams, by using a set of several rotating disc with inscribed symbols, which directly interact with the locking mechanism or through an electronic or mechanical keypad. In 1206, the Muslim engineer Al-jazari documented a combination lock in his book al-Ilm Wal-Amal al-Nafi Fi Sina’at al-Hiyal (the Book of knowledge of ingenious Mechanical Devices) [14].

In 1954, Dee Horton and Lew Hewitt invented an automatic sliding gate known as Horton automatic which uses number of symbols for the open and close operation. [15] The idea was targeted to circumvent problems of swing gates. In 2002, Dee Horton and Lew Hewitt propounded the use of enhanced four (4) digit alarm keypad using buffer and CMOS.

Progressively, RFID technology was incorporated as a security measure. [4] Relayed challenges and issues facing the technology. The RFID tags were prone to various physical and virtual attacks upon the system. The second concern stems from the need of privacy surrounding the data collected as observations recorded can be used for breaches in privacy. The last issue was that: data collected among systems in particular where passive tags were utilized, produces data characteristics that makes the system harder to use.


Infrared OTP technology was used for smart door locks operated by smart phones in the research presented by [11]. Furthermore, [6] presented an enhanced model of [11] in his survey to improve the distance of usage of his innovation based on Internet of things (IoT).

A. Desired Improvement

The OTP system which utilizes GSM technology with central coordination of a microcontroller, will eliminate challenges of mechanical complexities in lock systems presented by [14], reduce human involvement and use of discreet component presented by [15], cushion challenges of RFID technology presented by [4], extirpate limited range of application of Bluetooth and infrared technology accounted by [5] and [3] respectively.

Furthermore, making security access private in biometric centered lock systems. Finally, the OTP innovation will create a framework for meshing together other security based systems

III. DESIGN METHODOLOGY

There is always a ground laying foundational approach towards any innovation. In the context of this research, the system’s architecture was segmented into software and hardware makeups in other to enforce simplicity and extirpate complexities at output. Technically, the hardware segment was aimed at mapping out the physical connections of the components used in the implementation. The block diagram shown in Fig.1 gave the hardware orientation of the system.

The software design which was drawn from interpretation of the flowchart, was used to control the hardware of the system. Software simulation of the innovation was done using Proteus to determine physical workability of the project. Set of instructions mirroring the flowchart was written in the Arduino IDE as part of the software design. The written codes was transferred to the microcontroller (ATMEGA 328p) using the Arduino development board via a USB cable.
A. Hardware Selection Criteria

The ATMEGA328p is a high-performance Atmel’s 8-bit microcontroller. It is a low-power, high-performance based microcontroller which combines 32KB (kilobyte) ISP (in-system programming) flash memory with read-while-write capabilities, 1KB EEPROM (electrically erasable programmable read-only memory), 2KB SRAM (static random-access memory), 23 general purpose I/O (input/output) lines, 32 general purpose working registers, a single 16-bit Timer/Counter with independent prescaler, compare and capture modes.

Other core features of the ATMEGA328p microcontroller are wide operating voltage range: 1.8V to 5.5V, maximum operating frequency of 20 MHZ, data retention for 20 years at 85°C and 100 years at 25°C and 10 bit, 6 channel analog to digital Converter. With these unique features, the ATMEGA328p was preferred for the project [2]. The ease of programming, simplicity and portability gives the microcontroller added advantage.

Other hardware makeups of the implementation such as keypad, GSM module, LCD and door driver circuitry were selected based on the ease of interfacing them to the microcontroller’s input/output port, portability and individual technological advancement. In this construction, a four by four matrix keypad was used. The model for the GSM module was SIM800L while a sixteen by two model was used as the LCD. Lastly, the door driver circuitry was a makeup of transistor for current amplification, a relay for actuating the door and diode to protect the transistor from spikes.

B. Power Supply Design.

The power supply design was responsible for converting ac voltage to dc voltage. LM317, LM7805, and LM7812 voltage regulators were used to obtain a 4.20V, 5V 12V respectively.

C. Shunt Capacitor $C_1$ Numeric Design

The peak voltage is $V_{peak} = V_s \times \sqrt{2}$ (1)

The peak voltage is the difference between the positive peak voltage waveform and the negative peak voltage waveform of the transformer secondary ac signal [1].

$V_s = 15V$ (Rating of the secondary voltage of the transformer used)

$V_{peak} = \sqrt{2} \times 15 = 21.21V$

value of the rectified voltage $= V_{dc} = \frac{2}{\pi} V_{peak}$ (2)

The dc value $V_{dc}$ of the rectified voltage was calculated using (2)

$V_{dc} = \frac{2}{\pi} \times 21.21 = 13.50V$

Maximum load current is given by $I_m = \sqrt{2} \times I_{RMS}$ (3)

The maximum load current is the maximum current the loads in the implementation can actually demand from the system’s power supply unit [1].
\[ I_{R,M.S} = 500mA = 0.5A \text{ (Rating of the secondary current of the transformer used)} \]

The maximum current the circuit loads can draw from the power supply was calculated using (3)
\[ I_m = \sqrt{2} \times 0.5 = 0.71A \]

Average load current \( I_{dc} = \frac{2}{\pi} I_m \) \hspace{1cm} (4)

The average load current was calculated using (4)
\[ I_{dc} = \frac{2}{\pi} \times 0.71 = 0.45A \]

It was preferable to use a filtering capacitor that will hold the peak ripple voltage \( (V_{\text{ripple}}) \) at approximately 1%. The ripple factor (RF) was important in deciding the effectiveness of the rectifier. That is, it indicated how much rejection the rectifier had to have in order to achieve a certain noise level on the output [1].

**Peak ripple voltage \( (V_{\text{ripple}}) \) = RF × \( V_{dc} \) \hspace{1cm} (5)**

\[ RF = \text{Ripple factor} = 1\% = 0.01 \]

The peak ripple voltage was calculated using (5)

**Peak ripple voltage \( (V_{\text{ripple}}) \) = 0.01 × 13.51 = 0.135V**

\[ C_1 = \frac{I_{dc}}{F \times V_{\text{ripple}} \times 4 \sqrt{3}} \hspace{1cm} (6) \]

\[ F = \text{Frequency of the source alternating current} = 50Hz \]

The shunt capacitor \( C_1 \) value was calculated using (6)
\[ C_1 = \frac{0.45}{50 \times 0.135 \times 4 \sqrt{3}} = \frac{0.45}{46.76} = 0.009624F \]
\[ C_1 = 9624\mu F \]

From the E series for capacitors available in commercial purchase, the rated capacitance for \( C_1 \) was not available. Hence, a slightly higher capacitor of 10,000\( \mu F \) was used. The higher the capacitance value above \( C_1 \), the better its filtering capacity

Applying KVL across the LED (D1) loop, with source voltage from LM7805, (7) was obtained
\[ V = V_D + I_D R_4 \hspace{1cm} (7) \]
\[ V = 5V \text{ (Source voltage of the LED)} \]
\[ V_D = 2V \text{ (Voltage consumed by D1 from its data sheet specification)} \]
\[ I_D = 20mA \text{ (Current consumed by D1 from its data sheet specification)} \]

From (7)
\[ R_1 = \frac{V - V_D}{I_D} = \frac{5 - 2}{20mA} = \frac{3}{20} = 150 \text{ ohms} \]

Applying KVL across the LED (D1) loop, with source voltage from LM7812, (8) was obtained
\[ V = V_D + I_D R_4 \hspace{1cm} (8) \]
\[ V = 12V \text{ (Source voltage of the LED)} \]
\[ V_D = 2V \text{ (Voltage consumed by D1 from its data sheet specification)} \]
\[ I_D = 20mA \text{ (Current consumed by D1 from its data sheet specifications)} \]

From (8)
\[ R_1 = \frac{V - V_D}{I_D} = \frac{12 - 2}{20mA} = \frac{10}{20} = 500 \text{ ohms} \]

(9) is a standard formula from the data sheet of LM317 used to calculate required output voltage from the regulator
\[ V_{max} = V_{\text{ref}} \left( 1 + \frac{R_2}{R_3} \right) \hspace{1cm} (9) \]

\[ V_{max} = \text{Required voltage from LM317 = 4.2V} \]
\[ V_{\text{ref}} = \text{LM317 reference voltage from data sheet = 1.25V} \]

Setting \( R_3 \) as 220 ohm, then (9) becomes
\[ 1.25 \times \left( 1 + \frac{R_2}{220} \right) = 4.2 \]
\[ R_2 = \frac{1.25 \times 4.2}{220} \]
\[ 924 = 275 + 1.250R_2 \]
\[ 924 - 275 = 649 = 1.25R_2 \]
\[ \frac{649}{1.25} = R_2 = 519.2 \text{ Ohms} \]

Commercially, an exact rating of a 519.2 Ohm value resistor is not obtainable. Hence, a variable resistor of 1k Ohms was used.
D. Design of LCD Constant Divider

The LCD constant divider are used to establish the brightness level or contrast of the LCD. The constant divider was used as an improvisation to the use of potentiometers.

\[
V_{OUT} = \frac{R_1}{R_1 + R_2} \times V_{CC} \tag{10}
\]

\( R_1 = 10k \text{ Ohms. This resistor was chosen for convenience in calculating } R_2 \)

\( V_{CC} = 5V. \text{ Voltage source for the LCD.} \)

\( V_{OUT} = 4.5V. \text{ Voltage needed to establish the brightness of the LCD} \)

From (10)

\[
4.5 = \frac{10000}{10000 + R_2} \times 5
\]

\[
50000 = 45000 + 4.5R_2
\]

\[
50000 - 45000 = 4.5R_2 = 5000
\]

\[
R_2 = \frac{5000}{4.5} = 1111.11 \text{ Ohms}
\]

\( R_2 = 1111.11 \text{ Ohms} \)

The numerical value of resistor \( R_2 \) is not available for commercial purchase. Hence, a resistor of 1K ohms was used in its stead.

E. Microcontroller’s Clock Circuitry Design.

Every microcontroller needs a clock source. Clock signals are everywhere inside a microcontroller. Clocks govern the speed at which the processor executes instructions, the baud rate of serial-communication signals, the amount of time needed to perform an analog-to-digital conversion and so much more. When you need seriously high precision and stability without the additional cost of a crystal-based oscillator IC (integrated circuit), opt for the standalone crystal approach. [8]. In Fig 5. Capacitor \( C_1, C_2 \) and the 16MHz crystal oscillator, set up the clock circuitry

Since high precision and stability was needed without additional cost of a crystal-based oscillator IC, a standalone crystal approach was utilized using a 16MHz crystal oscillator with total load capacitance (\( C_{L_{\text{TOTAL}}} \)) of 16pf

\[
C_{L_{\text{TOTAL}}} = 16pf
\]

\[
C_{L_{\text{TOTAL}}} = \frac{C_1 \times C_2}{C_1 + C_2} + C_P \tag{11}
\]

\[
C_1 = C_2 \tag{12}
\]

\( C_p = \text{Stray capacitance. It is guestimated to be in the neighborhood of 2-5pf. [16]} \)

Stray capacitance is unintended and unwanted capacitance in a circuit [17].

\( C_1 \) and \( C_2 \) are identical capacitors used to stabilize the clock frequency

Substituting (12) in (11) then, (13) was obtained

\[
C_{L_{\text{TOTAL}}} - C_P = \frac{C_1}{2} \tag{13}
\]

From (13), choosing \( C_P = 5pf \)

\[
16 - 5 = \frac{C_1}{2}
\]

\( C_1 = C_2 = 22PF \)

F. Door Driver Circuitry Design

The door driver circuitry was used to actuate the doors to open or to close after receiving pulse command from the
microcontroller via the transistor. A transistor was used as a current amplifier since the current from the microcontroller was not sufficient to switch the relay for driving the doors.

\[ I_{b_{min}} = \frac{I_{c_{sat}}}{h_{fe}} \]  

(14)

\( h_{fe} \) = 110 Amplification factor for the transistor according to its data sheet.

\( I_{c_{sat}} \) = 100mA (collector current to drive the transistor to saturation according to data sheet).

\( I_{b_{min}} \) = Minimum base current

From (14)

\[ I_{b_{min}} = \frac{I_{c_{sat}}}{h_{fe}} = \frac{100mA}{110} = 0.91mA \]

\[ R_2 = \frac{V_{cc} - V_{BE}}{I_{b_{min}}} \]  

(15)

\( V_{cc} \) = (Base voltage of the transistor feed from the microcontroller’s port)

\( V_{BE} \) = (Base emitter voltage of the transistor from its data sheet)

From (15)

\[ 5 - 0.7 = 4.72523 \approx 4.7k \text{ Ohm} \]

Applying KVL across the LED loop, (16) was obtained

\[ V = V_D + I_D R_1 \]  

(16)

\( V\) = 12V (Source voltage of the LED)

\( V_D \) = 2V (Voltage consumed by the LED from its data sheet specification)

\( I_D \) = 20mA (Current consumed by the LED from its data sheet specifications)

From (16)

\[ R_1 = \frac{V - V_D}{I_D} = \frac{12 - 2}{20mA} = \frac{10}{20} = 500 \text{ ohms} \]
IV. TEST RESULT

Testing of the project was a means of validating whether the objectives and purpose of the project were achieved.

Table 1: Door security test results

<table>
<thead>
<tr>
<th>No.</th>
<th>Status</th>
<th>Approved</th>
<th>Number</th>
<th>OTP Received</th>
<th>DC Motor</th>
<th>FinalDoorState</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System</td>
<td>OTP Valid</td>
<td>Yes</td>
<td>Yes</td>
<td>HIGH</td>
<td>Opened</td>
</tr>
<tr>
<td>2</td>
<td>System</td>
<td>OTP Valid</td>
<td>Yes</td>
<td>No</td>
<td>LOW</td>
<td>Closed</td>
</tr>
<tr>
<td>3</td>
<td>System</td>
<td>OTP Invalid</td>
<td>Yes</td>
<td>Yes</td>
<td>HIGH</td>
<td>Opened</td>
</tr>
</tbody>
</table>

V. CONCLUSION

From the results obtained, it was glaring that access through the door was only permitted if the right user identification was initially inputted, followed by authentication of the OTP sent. The system proved that security access to the building can be handled privately. Furthermore, the unutilized input/output port of the microcontroller provided means of integrating other security enhancement mechanisms like cameras, biometrics, Bluetooth, and RFID technologies.
accommodate the physically challenged and illiterates who may be users of the building where the project can be incorporated. The little drawback to this enhancement method is that update needs to be made on the already written software programme by a skilled professional so as to control the added security measures. Lastly, the project will not be useful in application in areas void of mobile network

ACKNOWLEDGMENT

In awe, the project team is appreciative to both the Department of Electrical/Electronic Engineering and Computer/Communication Engineering, both of Abubakar Tafawa Balewa University Bauchi State, Nigeria, for her fundamental academic trainings during undergraduate studies and also warm reception tendered to the project team during the buildup stages of the innovation. Nascomsoft Embedded is not left out as her contributory wealth of experience was pivotal to the actualization of the project. The team can’t keep shut without blowing the trumpet in appreciation to the works in prints of predecessors of similar projects whose details are honored in the reference section

REFERENCES


DOI: http://dx.doi.org/10.24018/ejerce.2020.4.3.220
Uko Victor Sorochi obtained his B.Eng. in Electrical/Electronic Engineering from Abubakar Tafawa Balewa University Bauchi State, Nigeria in 2018. His research interests are in embedded systems, amplifier designs and energy systems. Mr. Victor is an associate member of Nigeria Society of Engineers, Environment and Safety Management Institute, and Chartered Institute of Contract Project and Facility Management. His alter ego include, but are not limited to: guest poster, sustainable development advocate, graphics designer and creative writer. Mr. Victor is currently with the Works and Service Department of the University of Port Harcourt, Nigeria.

Isa Abdulrauf Inusa obtained his B.Eng in Computer and Communications Engineering from the prestigious Abubakar Tafawa Balewa University Bauchi State, Nigeria in 2020. His research interests are in embedded systems and communication systems. He currently marshals expertise in web design and development as a corps member.

Nasiru Abdulsalam obtained his B.Eng. in Computer and Communication Engineering from Abubakar Tafawa Balewa University Bauchi State, Nigeria in 2018. His research interests are in embedded systems and wireless sensor networks. Mr. Nasiru is a tech savvy who doubles as the founder and CEO of Nascomsoft Embedded. An enterprise with mind blowing technological approaches to surmount human and environmental challenges.