IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Smart Home Security Analysis Using Microcontroller

Arjun S[1], GopiKrishna V[2], Gowtham B[3], Siddharthan B[4], Dr. V. Manikandan, M.E.,Ph.D.,[5]

[1,2,3,4]Department of EEE, Coimbatore Institute of Technology, Affiliated by Anna University, Coimbatore, Tamil Nadu, India.

[5]Professor at Department of EEE, Coimbatore Institute of Technology, Affiliated by Anna University, Coimbatore, Tamil Nadu, India.

E-mail: [1]1903065eee@cit.edu.in, [2]1903075eee@cit.edu.in, [3]1903077eee@cit.edu.in, [4]1903103@cit.edu.in, [5]manikandan@cit.edu.in

Abstract

To prevent data theft, unauthorized access, and network misuse, data modification network security plays a major role in it. Another important role is preventing DOS (Denial Of Service) attacks and making sure of uninterrupted service for legal network users. Network Security also has some defense protocols to protect the data from internal and external attacks.

The proposed work is based on creating a safe and secure network by creating a double authentication i.e., by using mail and SMS. Double authentication can also be used in banks as many thefts are being done in a single authentication, if double authentication is implemented through SMS and mail it provides additional security for transactions that are done online. This research is implemented with the help of servers and a microcontroller to develop an application that is essential in a smart home design.

Keywords: Microcontroller, Cybersecurity, smart home, authentication.

1. Introduction

The process of protecting electronic systems, networks, computers, servers, mobile devices, and data from malicious attacks is known as cyber security. This domain includes all technology that accumulates data, Converts, or transfers in all devices, that are, connected to it. All devices which produce data has to be protected with Firewall, Ransomware protection, DOS protection, Monitoring, etc. In addition to it information technology should provide

DOI: https://doi.org/10.36548/jsws.2023.2.003
Received: 31.04.2023, received in revised form: 31.05.2023, accepted: 09.06.2023, published: 19.06.2023

security from theft of assets, [assets generally include hardware such as servers and Switches and Software such as applications and confidential information] Cyberextortion [use of various tactics, such as phishing, Injection & Malware, holding victim's data for ransom], Identity theft [It happens when someone tries to steal your information/patron to commit fraud], loss of privacy [occurs as an act of entering the device and takes attempts to have control over it], etc., Nowadays cybersecurity plays a major part in industries. Nearly billions of dollars are spent annually on cyber security since no device is immune from attacks or it is completely secure. Cyberattacks keep on raising day by day, today technology provides us with more advantages and disadvantages, and people who tend to misuse it are the greatest threat to privacy. • when the breaching happens, it can provide great loss by affecting the consumer and providers. The most famous cybersecurity is the Yahoo cyberattack, in this attack over 500 Million accounts were compromised. Phishing attacks are the most widespread and damaging attack that attacks small-scale industries. Phishing refers to an attempt to steal sensitive data Mostly in form of login credentials, credit card numbers, bank account numbers, etc ., to sell or use it for their benefit. In cyber security, Multi-Factor Authentication (MFA) is very important in reducing the risk factor, this provides an extra layer of security for the devices. Device hijacking occurs mostly when home devices are breached. These devices have little or no built-in security. Those can be prevented by providing certain securities or following certain steps such as using a unique password for every device which are connected. etc.,

1.1 Overview

The proposed system provides a server-based security system that reduces the number of intruders who try to access the system by providing a request access form and an admin form. With the admin form, the user takes full control of the system and will be provided with alert messages when misused. The slave trying to access the system will provide his credentials in the request access form.

1.2 Objective

The objective is to provide a multi-factor authentication system using SMS and Mail with the help of a mini webserver using the necessary PHP code and to implement this security system with the help of microcontrollers in home automation. The mini web server created must be user-friendly and issues approval to other systems.

2. Literature Review

2.1 "Improving Home Automation Security; integrating device fingerprint into Smart Home"

This study outlines the significance of modern smart home internet connection and explores its numerous security concerns. It also describes the development of the idea of device fingerprinting. In this study, a two-stage method for smart homes that uses biometrics and login credentials is proposed.

2.2 "Home automation and security system with Node MCU using Internet of Things"

The general operation of IoT-based sensor systems is covered in this paper. The prototype used here employs a Node MCU connected to the internet and is controlled by an Android or iOS smartphone. As a microweb server and an interface for hardware modules, Node MCU operates. The system's ability to detect intrusions using motion sensors is another important feature.

2.3 "Review and performance analysis on wireless Smart Home and Home automation using IOT"

An technique for home automation via the Internet of Things is provided by this research effort. With this approach, we use a webpage to remotely control our home appliances from our computers or mobile devices. The internet and IoT make it possible to automate homes anywhere in the globe, raising living standards.

2.4 "Automatic service request system for security in smart home using IoT"

The Raspberry Pi automatic service request system for smart home security, which is connected to the cloud via the internet utilising the wireless network, is discussed in this paper along with IoT. This system primarily uses several sensors for home monitoring.

2.5 "Towards residential smart grid: A practical design of wireless sensor network and mini-web server based low-cost home energy monitoring system"

In order to create a smart grid system in a residential setting, this paper describes the Wireless Sensor Network (WSN). A WSN and a small-scale web server-based monitoring system that primarily focuses on cheap energy are also described.

2.6 "IOT enabled smart lighting systems for smart cities"

This paper discusses the importance of IOT in smart cities and integrates it with different domains for seamless operation. It mainly discusses integrated lighting systems with advanced sensors to obtain and efficiently manage smart lighting systems.

3. Basic Working Methodology

The system's hardware and web servers should be connected to a common network. Initially, the web page is opened and the mail id and number are given to become the slave. A 4-digit OTP is sent to mobile as SMS and mail id. The OTP is entered in the required box on the web page. The slave will be accepted by the master. Now the master can add as many slaves with this operation. The slaves can also be modified by the master. Now another webpage loads right after the OTP is entered. This allows the access for the slave node to access the devices. For critical devices such as lockers, a separate message is sent to the master that the locker is opened to ensure safety. Each and every action of slaves are sent as messages to the master except for non-critical devices such as fans, lights, Etc.,

3.1 Components Used

A. NODEMCU ESP8266

NODEMCU is an open-source IOT platform. Its operating voltage is 3.3v. It has a RAM of 32kb to store the coding provided by the user. a flash memory of about 16k maximum is also attached to the device. A Micro USB slot is provided to feed the necessary code to the microcontroller. This primarily uses TCP/UDP communication protocol for connecting to the server.

B. LCD With I^2C

The LCD display is used along with the integrated circuit in order to reduce the number of pins connected to the Arduino. The LCD display here used is a 16x2 display, the backlight is green and the character color is black. The integrated circuit has the interfacing address of 0x20 to 0x27. The integrated circuit is interfaced at the back of the LCD display. The information is displayed using the LCD.

C. Single Relay Module

The Relay module is a board that can be used to control high voltage and high current devices. This module is designed to interface with other microcontrollers. This module is compatible with any 5v microcontroller. It is also used in safety circuits. A terminal block will be provided with the module for connection purposes.

D. SIMCOM GSM (SIM900a)

GSM module offers GPRS/GSM technology for communication with the use of a mobile sim. This module allows users to send and receive mobile calls and SMS. This module can be programmed using Arduino IDE software. This module provides antenna support This Dual Band GSM/GPRS engine SIM900A GSM Modem Module with SMA Antenna operates at frequencies of 900 MHz and 1800 MHz. The modem has an RS232 interface that enables you to link a microcontroller with an RS232 chip (MAX232) and a PC. With the help of the AT command, the baud rate can be changed from 9600 to 115200. This enables to connect with the internet through GPRS, the GSM/GPRS Modem has an inbuilt TCP/IP stack. It is appropriate for applications involving data transfer, voice calls, and SMS in M2M interfaces. Through straightforward AT commands, the modem is used to make audio calls, send and receive SMS, answer incoming calls, access the internet, and more. The terminals rx and tx are mainly used for text messages and calling purposes.

3.2 Working

A. Smarthome System

Here a basic smart home system is provided using an LED and a fan which are connected to the NODEMCU which acts as a server. The GSM module is provided with a SIM card so it can connect to the network. Common SSID is programmed into NODEMCU so that the system automatically connects to that network when available. LCD shows the current status of the system.

B. Request Access Form

This form is for the person accessing the system. It is coded in such a way that he must enter his credentials and request access to the user. Once the access is granted the user will receive OTP in both SMS and mail to access the system. If entered correctly it grants permission to access the system.

C. Admin Form

This form is only for admins. Admin can access this form by connecting to the same network as the hardware. The admin has to enter the IP address shown in the LCD display in order to connect to the hardware. Here the admin can monitor the system and can grant or deny access to others.

D. Block diagram

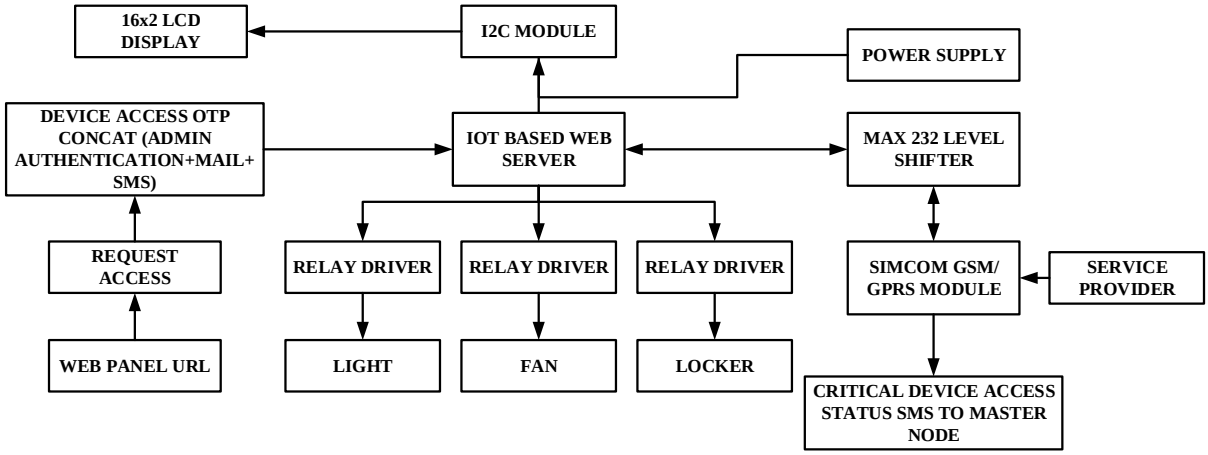

Figure 1. Block Diagram

The above Fig 1 explains the research methodology followed . as shown in the fig.1 the main control is done using the server. User information is feed to the server. For others to access the system the user provides a double authentication system by providing OTP through mail and SMS. This is sent using the GSM module provided. If critical devices are accessed, an alert message will be given to the user.

4. Results and Discussion

A. Hardware Result

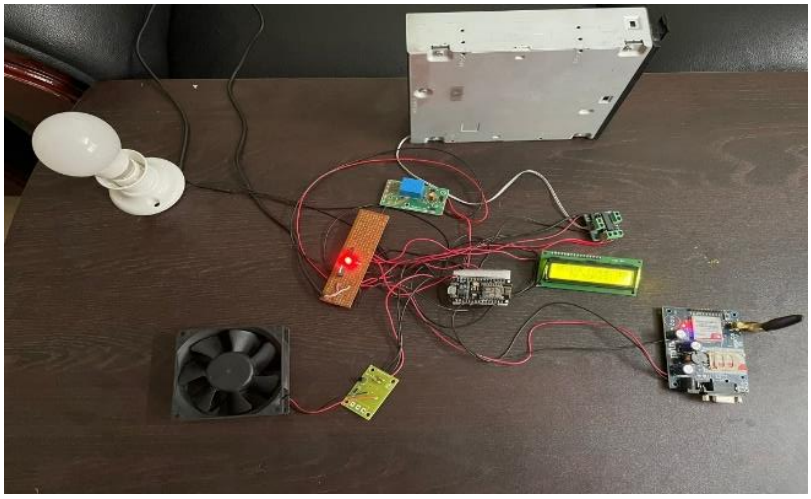

Figure 2. Hardware

Fig 2 shows the completed hardware. When the supply is provided the LCD backlight turns ON and the device is connected to the provided SSID. The GSM module connects to the network with the help of the antenna provided.

B. Request Access Form

The mini webserver for the proposed work was developed with the PHP using the HTML and the CSS reference. The database of the system is managed with the help of the Sybase. The PHP is commonly preferred with server that extends communication between the frontend and the backend.

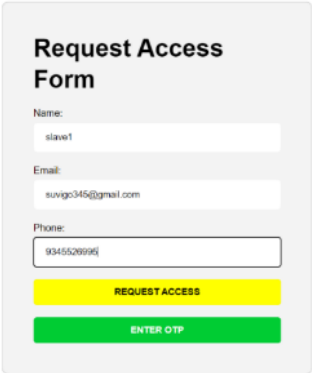

Figure 3. Access Form

This form is provided to the slave to access the system. The slave has to provide his credentials to access the system. The slave must enter his Name, Email, and mobile number to receive the OTP from the master node. Figure 3 shows the layout of the access form.

C. Admin Form

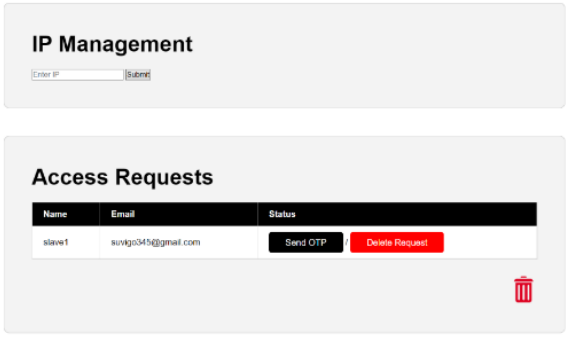

Figure 4. Admin Form

Figure 4 shows the admin form. Admin is provided with his login credentials. After entering his data, the admin enters the network IP address. All the requests sent by the slave can be viewed by the admin who can approve or deny the request. This is how the admin controls the whole system.

D. Mobile Sms and Email

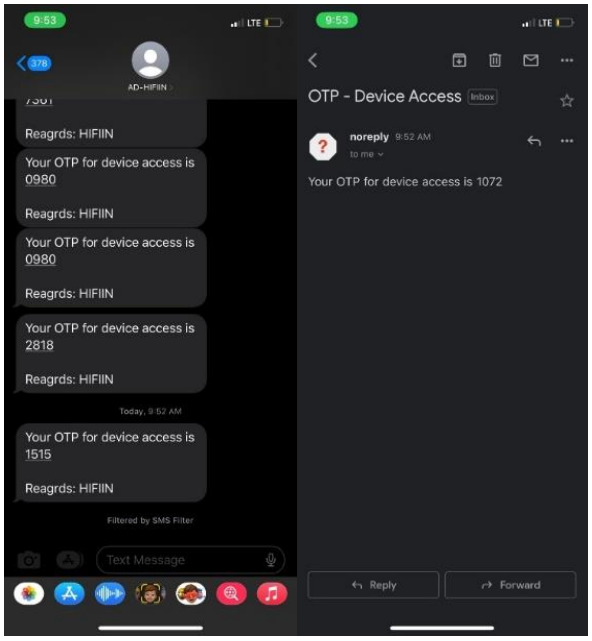

Figure 5. SMS and Email

When the master decides to send OTP it will be sent with the help of the GSM 900a module and the slave can enter these randomly generated pins to gain access. Figure 4 shows the OTP sent to the slave's credentials.

E. OTP Form

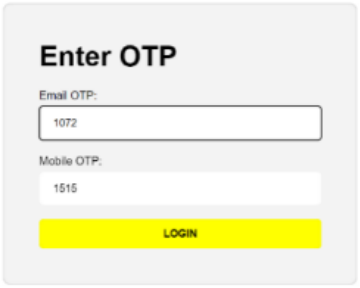

Figure 6. OTP Form for the Slave Node

By entering the correct OTP he can access the system. If the wrong OTP is entered then an alert signal will be sent to the master. If entered right. The right OTP entered allows the slave to access the system.

5. Conclusion

5.1 Conclusion

Nowadays, more people are preferring smart homes, the research objective is to provide a security system with high security like two-factor authentication and this authentication will be accessed only by the admin. In this way every user will get a unique code, so intruders cannot access it with the help of the app or the same server-based security system, in this way the research tries to provide the users a security system at an economical price. Cyber security is one of the most important factors in the growing digital world. The threats of it are hard to stop, so it is important to learn how to defend or resist them.

5.2 Future Scope

This system can be used in many different sectors in addition to Smart Homes. More thefts can be prevented by giving the master node complete access, and intruders will find it difficult to break into the system. The majority of authentication systems used for web-based applications rely on traditional username and password-based schemes, which are easily

vulnerable to attack. Various sophisticated user authentication schemes are currently evolving, all of which are based on sophisticated encryption methodologies.

References

[1] Arun Cyril Jose, Reza Malekian, and Ning Ye, “Improving Home Automation Security; integrating device fingerprint into Smart Home,” IEEE Access, Volume 4, pp.5776-5787, 2016.

[2] K. Lova Raju, V. Chandrani, SK. Shahina Begum, M. Pravallika Devi, “Home automation and security system with Node MCU using Internet of things,” Proceedings of IEEE International Conference on Vision towards emerging trends in communication and networking (ViTECoN), 30-31 March, Vellore, India, 2019.

[3] Kabita Agarwal, Arun Agarwal, Gourav Misra, “Review and performance analysis on wireless Smart Home and Home automation using IOT,” Proceedings of IEEE 3rd International conference on I-SMAC (IOT in Social, Mobile, Analytics, and Cloud), 12-15 December, Palladam, India, INSPEC-19452282, 2019.

[4] Pranav Kumar Madupu, B Karthikeyan, “Automatic service request system for security in smart home using IoT,” Proceedings of IEEE 2nd International Conference on Electronics, communication and aerospace technology(ICECA), 29-31 March, Coimbatore, India, 2018.

[5] Minh-Thanh Vo, Minh-Triet Nguyen, Tuan-Duc Nguyen, Chi-Thong le, Huu-Tue Huynh, "Towards residential smart grid: A practical design o wireless sensor network and mini-web server based low-cost home energy monitoring system" Proceedings of IEEE International Conference on Advanced Technologies for Communications (ATC), 16-18 October 2013, Ho Chi Minh City, Vietnam.

[6] A.K. Sikder, A.Acar, H.Aksu, K.Akkaya, M.Conti, “IOT enabled smart lighting systems for smart cities,” Proceedings of IEEE 8th Annual Computing and Communication Workshop and Conference(CCWC), Las Vegas, USA, pp.639-645, 2018.

[7] Mowad, Mohamed Abd El-Latif, Ahmed Fathy, and Ahmed Hafez. "Smart home automated control system using android application and microcontroller." International Journal of Scientific & Engineering Research 5, no. 5 (2014): 935-939.

[8] Isa, Eleni, and Nicolas Sklavos. "Smart Home Automation: GSM Security System Design & Implementation." *Journal of Engineering Science & Technology Review* 10, no. 3 (2017).

[9] Agosta, Giovanni, Alessio Antonini, Alessandro Barenghi, Dario Galeri, and Gerardo Pelosi. "Cyber-security analysis and evaluation for smart home management solutions." In *2015 International Carnahan Conference on Security Technology (ICCST)*, pp. 1-6. IEEE, 2015.

[10] Gunge, Vaishnavi S., and Pratibha S. Yalagi. "Smart home automation: a literature review." *International Journal of Computer Applications* 975, no. 8887-8891 (2016).

Author's Biography

Arjun S is currently pursuing his final year BE-Electrical and Electronics Engineering at Coimbatore Institute of Technology, Coimbatore, Tamil Nadu. His research area of interest includes Cybersecurity and Digital Electronics.

Gopi Krishna V is currently pursuing his final year BE-Electrical and Electronics Engineering at Coimbatore Institute of Technology, Coimbatore, Tamil Nadu. His research area of interest includes Digital Electronics and Embedded systems.

Gowtham B is pursuing his final year BE-Electrical and Electronics Engineering at Coimbatore Institute of Technology, Coimbatore, Tamil Nadu. His research area of interest includes Internet of Things and Digital Electronics.

Siddharthan B is pursuing his final year BE-Electrical and Electronics Engineering at Coimbatore Institute of Technology, Coimbatore, Tamil Nadu. His research area of interest includes Internet of Things and Cybersecurity

Dr. V. Manikandan is currently working as a Professor in the Department of Electrical and Electronics Engineering at Coimbatore Institute of Technology, Coimbatore. He obtained his doctoral degree from Anna University, Chennai. He did his masters in Applied Electronics at PSG College of Technology, Coimbatore, and his Bachelor's degree in Electrical and Electronics Engineering at Government College of Technology, Coimbatore. He is also guiding researchers in the area of Soft Computing.