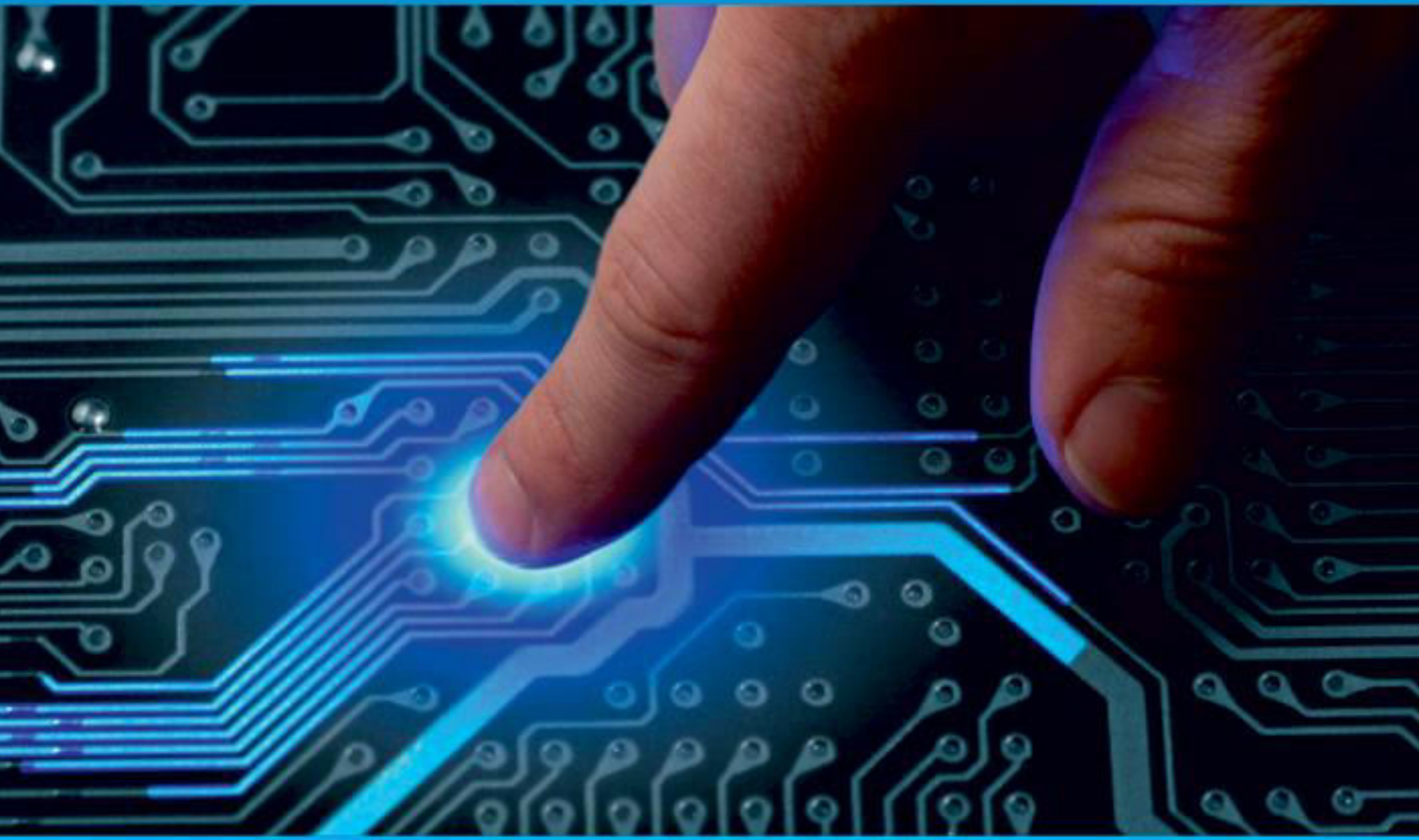
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005328 |

Prevent Vulnerability from Intruder Using IOT

Ms.B.Manjubashini M.E., Prasanth.S, Srithannu.K, Boobalan.G, Dinesh.P

Assistant Professor, Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

ABSTRACT: The Internet of Things plays a key role in digital transformation. Information security and privacy issues related to IoT devices have attracted global attention, because of the ability of these devices to interact with the physical world. IoT vulnerabilities continue to emerge, making it critical for manufacturers to emphasize IoT security by design. IoT vulnerabilit ies have been discovered and exposed across many industries. These vulnerabilities threaten sensitive data as well as personal safety. But in domestic cases like smart home its not economically possible to high end security devices. A topology must exist to prevent IoT devicesin domestic applications from intruders at low cost. By analyzing existing topologies and its vulnerabilities, the information obtained from them is used to develop a new topology to protect user's IoT devices from unknown person or hackers. The new topology must adhere to all aspects of CIA triad.

I. INTRODUCTION

Every electronic device in the world can be intrude or hacked. However, in many organizational and domestic cases, people realize that they already have a large fleet of legacy IoT devices that have been gradually deployed over the years. Security experts have warned of the potential risk of large numbers of unsecured devices connecting to the Internet since the IoT concept was first proposed in the late 1990s. Many organizations use paid cybersecurity services like VMware, RSA, Microsoft Cybersecurity Protection, Amazon Macie,etc. Some organizations use their own cybersecurity specialists and their own security devices. Even these developments in security didn't stop the intruder or hackers to exploit the organizations data. Incase of domestic applications, most of the current devices like laptops, computers and smartphones comes with built-in software firewalls and antivirus services which is a basic level of security when compared with organization's security developments. IoT devices are even more vulnerable to cyber attacks like Physical attacks, Encryption attacks, Denial of Service(DoS), Firmware hijacking, Botnets, Man in the middle(MiTM), Ransomware, Eavesdropping. Privilege escalation, Brute force password attack, Cross Site Recovery Forgery(CSRF), etc. So there is a dire need of protection for IoT devices in domestic applications. Topologies like authentication and encryption can also be used to improve security. Analyzing the Existing one, the control of the system would be managed by user.

The purpose of the project entitled as "Prevent Vulnerability from Intruder" is to develop a topology to secure IoT devices in domestic applications like smart home to prevent Intruders or unknown person from data exploitation. This is achieved by using nodemcu . User will use various security methodologies like authentication and encryption to prevent hacker from exploiting the user.The user can have all access to prevent the data usage from unknown person through we set local IP address. On the way ,the protection will be given to home usage.. By analyzing existing topologies and its vulnerabilities, the information obtained from them is used to develop a new topology to protect user's IoT device from hackers. The new topology must adhere to all aspects of CIA triad.

II. LITERATURE REVIEW

Urvi Singh and MA Ansari entitled "Smart home automation System using IOT" in 2019 2nd International Conference on Power Energy, Environment and Intellige nt Control(PEEIC).This paper Highlights the IOT is the newest and rapid growth internet technology in recent times. The paper describes the ESP8266 demonstrated and used as a Wi-Fi technology. By using this, the multiple users in the home uses the sensors by using laptops and tablets. It is efficient use of technology and best usage for controlling the home devices and it provides the security for improving the safety.

SK Fahmida Islam, Md Iqramul Hasan, Morium Aktar and Mohammad Shorif Uddin entitled "Implementation and Analysis of an IOT-based home automation framework" in 2021 and this project approaches that the users to monitor and access the appliances in home and it is implement by using with low cost and user friendly IOT based using NodeMCU through mqtt protocol . This provides and support home safety, energy saving

Swati Swayamsiddha, Diptabtrata Mukherjee and Srinivas Ramavath entitiled "Home automation Using ESP8266 of IOT Module" in 2021. In this paper, using ESP8266 and IOT module automated the household electronics proposed. It said that the ESP8266 has the very cheap rate in the market. The IOT can connected and communicated by giving human commands using mobile, sensors and wireless. So, The voice instructors like Google Assistant are connected with the appliances.

Irene Joseph, Prasad B Honnavalli, BR Charanraj entitled "Detection of DoS Attacks on Wi-Fi Networks Using IOT sensors" in 2022. This paper gives the idea to prevent vulnerab le things with low cost . It describes the vulnerabilities, such as deauthentication attack, beacon flooding attacks are DoS attacks. The usage of ESP8266 Wi-Fi module is proposed. It can detect the attacks in wireless LAN . The main scope is to design the IOT network in a real time. So, This gives the idea to protect the unauthorized access from the intruder in a efficient way.

Prathmesh Shelke, Shubham Kulkarni, Swapnil Yelpale, Omkar Pawar et.al., entitled "A NodeMCU based home automation system" in 2018. This paper gives the idea of web browser uses to control the operated switches which is interfaced with nodeMCU and it has inbuilt Wi-Fi. The user can communicate with the processor through the browser and it is accessible remotely by the user. In this paper ,how the nodemcu process works and it implemented for smart homes and connections for the analog switch has to be power enabled or disabled.

Cristina Stolojescu-crisan, calin crisan and Bogdan-Petru Butunoi ., proposed the interconnecting sensors, actuators and other data sources. In this paper, the system is flexible and describe the qtoggle for application programming interfaces and the also represents the simple and common communication system. Most devices are based on ESP8266 and ESP8285 chips used by qtoggle .It allows the user to access the control of the system, sensors and it is user friendly, flexible and simplicity. The system is designed for access control and provides security for the home.

III. METHODS

INO - It is a software program created for use with arduino and it is used to provide required functionalities to the wi-fi module. In this project, INO scripts are used to connect to the wi- fi module, frontend functionalities like collection of credentials, service request and backend functionalities like service response, and other functions like authentication and encryption. The Arduino Electronics platform allows developers to create and install programs called sketches on different circuit boards.

Fig 1: Blockdiagram

The ESP8266 is acts as a Wi-Fi module for internet enabled device. We provide authentication and encryptions in ESP8266 using Arduino IDE. LED is used to indicate the changes in the state of the internet enabled devices due to hacker's involvement in the victim's network.

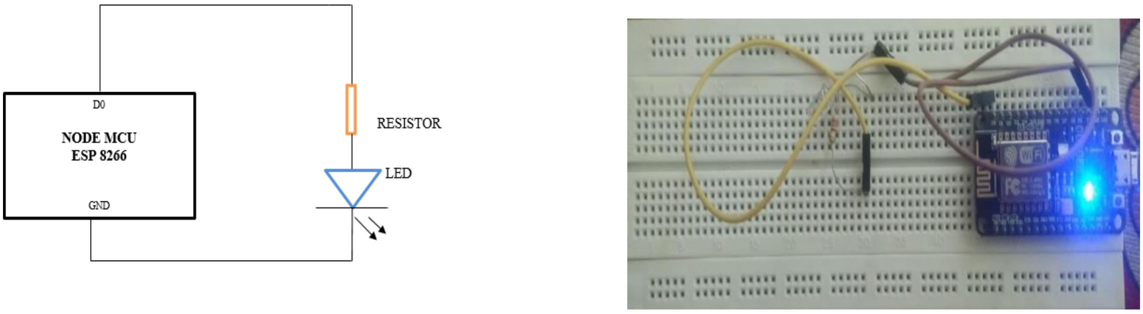
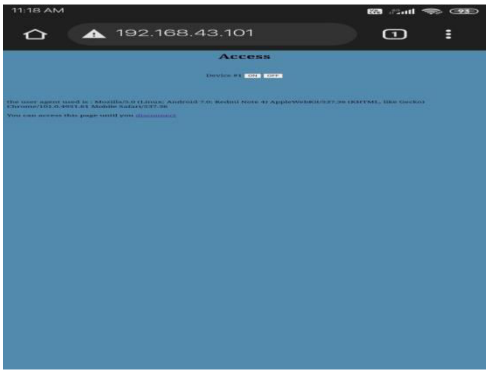


Fig 2: CIRCUIT DESIGN

The D0 or GPIO16 pin is connected to the resistor. The another end of the resistor is connected to the positive pin of the LED and the negative pin of the LED is connected to the GND pin of the ESP8266. A micro USB port is used to upload the source code and it also acts as a power supply to the module. Its always advised to use external power supply with voltage dropout regulatorbut due to uavailability, micro USB port is used. The source code is uploaded using Arduino IDE. To remove the program in the module RST button is used.

IV. RESULT ANALYSIS

Arduino was born at the Ivrea Interaction Design Institute as an easy tool for fast prototyping, aimed at students without a background in electronics and programming. As soon as it reached a wider community, the Arduino board started changing to adapt to new needs and challenge s, differentiating its offer from simple 8-bit boards to products for IoT applications, wearable, 3D printing, and embedded environments. All Arduino boards are completely open-source, empowering users to build them independently and eventually adapt them to their particula r needs. The software, too, is open-source, and it is growing through the contributions of users worldwide.



Access

Device #1 ON OFF

the user agent used is : Mozilla/5.0 (Linux; Android 7.0; Redmi Note 4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36

You can access this page until you disconnect

Fig3: Result analysis

V. CONCLUSION

The vulnerabilities in IoT devices during wireless mode were analyzed on various levels and the prevention scheme was established. Low cost and scalable network security for domestic IoT systems can be achieved. Each client session to access internet via an IoT device is protected and the connection is encrypted. A Domestic network of IoT devices can be protected from external threats without using high end network security devices like firewall, IDS or IPS.Real time implementation of authentication requires additional research works Privacy and personal data of the user can be protected. Using authentication most of the cyber attacks can be prevented at low cost. To implement in real time environments, we can develop the proposed topology in real time using a router and the Desktop. The Practical operation done in a environment using Arduino IDE.

REFERENCES

1. Abu MA, Nordin SF, Suboh et al (2018) Design and development of home security systems based on internet of things via favoriot platform. Int J Appl Eng Res 13(2):1253–1260.
2. Parihar, Y.S.: Internet of Things and Nodemcu. J. Emerg. Technol. Innovat. Res. 6(6), 1085 (2019)
3. W. Z. Guo, “Research on computer wireless network and information security,” Applied Mechanics and Materials, vol. 416-417, no. 1, pp. 1450–1453, 2013. Research on Computer Wireless Network and Information Security | Scientific.Net
4. R. Rana, “Man-in-the-Middle attack,” International Journal of Recent Advancement in Engineering & Research, vol. 1, no. 3, 2017. Man-in-the-Middle Attack to the HTTPS Protocol | IEEE Journals & Magazine | IEEE Xplore
5. Kristen S, “Cross Site Recovery Forgery”, Open Web Application Security Project(OWASP),2021.
6.Yogendra Singh Parihar, “Internet of Things and Nodemcu A review of use of Nodemcu ESP8266 in IoT products”, National Informatics Centre, (Mahoba(U.P.), India,2019).
7. Narang, S., Nalwa, T., Choudhury, T., Kashyap, N.: An efficient method for security measurement in internet of things. In: 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, pp. 319–323 (2018)
8. Kristiyanto Y, Ernastuti (2020) Analysis of deauthentication attack on IEEE 802.11 connectivity based on IoT technology using external penetration test. CommIT (Communication and Information Technology) J 14(1):5–51
9. Raghuprasad, Aswin (2020) Security analysis and prevention of attacks on IoT devices. In: 2020 international conference on communication and signal processing (ICCSP)

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details