INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 3 - V7I3-1935)
Available online at: https://www.ijariit.com

A Novel Approach of Preventing Cyber Attack on Industry 4.0

Gayatri Ravtole
gayatriravtole293@gmail.com
Bharati Vidyapeeth College of Engineering for Women, Pune University, Pune, Maharashtra

Anushika Pandita
anushikapandita12@gmail.com
Bharati Vidyapeeth College of Engineering for Women, Pune University, Pune, Maharashtra

Rajshree Ghatkar
rajshreeghatkar25@gmail.com
Bharati Vidyapeeth College of Engineering for Women, Pune University, Pune, Maharashtra

Rutuja Kamthe
rutujakamthe1312@gmail.com
Bharati Vidyapeeth College of Engineering for Women, Pune University, Pune, Maharashtra

ABSTRACT

The Internet of things (IoT) describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. The IoT concerns a wide range of modules like the data acquisition, communication, sensors etc.Owingtothe lack of consideration of cyber security threats, they have an inherent technical debt which results in compromised medical devices with unpredictable behaviour. With the increasing market share of the IoT devices in the healthcare field, it has offered a simple door for cyber criminals trying to misuse and profit from device vulnerabilities. In this paper we discussing about attack on smart bulb. We are providing cybersecurity on smart blub with different module such as attacking on smart bulb then detect the that particular attack last prevent the attack.

Keywords: *IoT, Zigbee, LED, Wires, Arduino, NodeMCU*

1. INTRODUCTION

The Internet of Things (IoT) is currently going through exponential growth, and some experts estimate that within the next five years more than fifty billion "things" will be connected to the internet. Most of them will be cheaply made sensors and actuators which are likely to be very insecure. This translates to multiple IoT and IIoT devices deployedwithinan organization. Such a setup increases the possibility ofthreats in spaces that had never posed cyber security risks before.IoT devices in these common spaces can have an effect on critical systems, like the intranet and In this project, IoT devices made by big companies with deep knowledge of security, which are protected by industry-standard cryptographic techniques, can be misused by hackers to create a new kind of attack: By using this new communication medium to spread infectious malware from one IoT device to all its physically adjacent neighbours, hackers can rapidly cause city-wide disruptions which are very difficult to stop and to investigate. Hence, we described an attack which has the potential to cause large scale effects. Moreover, fixing the malicious software update will require the physical replacement of every affected light bulb with a new one, and a waiting period for a software patch to be available before restoring light.

2. LITERATURE SURVEY

Fathima Jameset al. [5] proposed of IoT Cyber security based Smart Home Intrusion Prevention System device for Intrusion prevention system methodology based on three cyber security aspects congeniality, authentication, and access control and to overcome these attack surfaces, we introduced the risk analysis model which helps to choose a suitable mitigation strategy.

Changmin Lee al [0] proposed on Securing Smart Home: Technologies, Security Challenges, and Security Requirements.In this paper the security Challenges and threats to the existing solutions suited for smart homecare , homes, security threatsfrom each protocol layer and security requirements for smart home (User Authentication, Device Authentication, PhysicalProtection and Secure Key Management).

Razan AL MOGBIL,Salim EL Khedari al [3] IoT: Security Challenges and Issues of Smart Homes/Cities. For this weget information about security attack in IoT system(eg. Jamming attack, Tampering attack), real life Scenario (Jeep Cherokee Vehicle Attack) and security count measure are provided.

3. SYSTEM ARCHITECTURE

In this system we are developing the home automation light system with the help of Internet of Things and protecting it with providing se Home automation refers to the abilityofyour home to make its own decisions depending on environment conditions and give you the option to control it froma remote location. Above fig 1.1 is all about how we performing attack on IoT smart bulb devise and then detection willhappenover there at last we provide prevent attack that performingonsmart devise. .

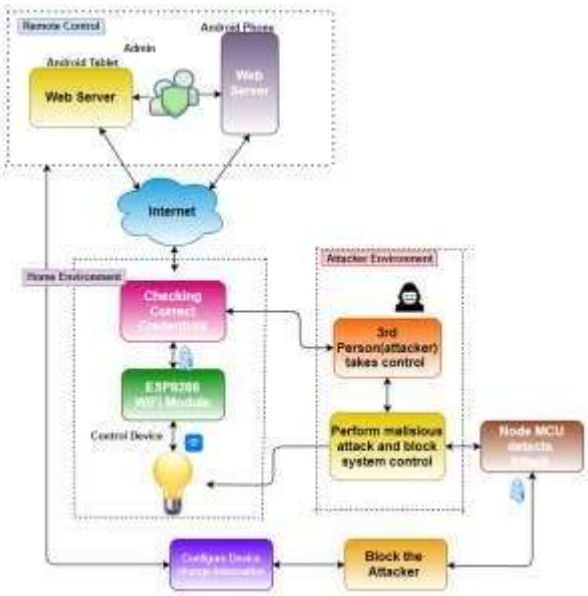

Fig. 1.1

Implementation

Home automation refers to the ability of your home to make its own decisions depending on environment conditions andgiveyou the option to control it froma remote location. In this systemwe are developing the home automation light system with thehelpof Internet of Things and protecting it by providing a secure mechanism. Here we have taken one Node MCU IDEESP8266as a Wi-Fi module It is an open source platformfor developing Wi- Fi based embedded systems and it is based on the popular ESP8266 Wi-Fi Module, running the Lua based Node MCU firmware. The project flow involves the control of Node MCU's GPIOs from a webpage on any device connected on the same network as the board. The status of the GPIOs control the coilsof the relays and that causes the relay to alternate between normaly open (NO) and normally closed (NC) condition depending onthe state of the GPIO, thus effectively turning the connectedappliance "ON" or "OFF". For doing this we need to connect Node MCUto the Arduino IDEwhich is software we are using for flashing the code into the Node MCU for performing actions on the device.
Here in the Code we have already given the SSID and PASSWORD i.e whatever we want from initially so only that password is used to make connection with the device.ESP8266WiFi.h library which allows the easy use of Wi-Fi functionalities of the board. It contains all we need to createor join a Wi-Fi access point and also create a server and clientwhich are all important for our project.

If the connection is successful, a text is printed on the serial monitor to indicate this, along with the IP address of the NodeMCU. This IP address becomes the web address for the server and should be entered on any web browser on the same network as the server so we are able to access it. And usersmove to the main server page which contains the ON and OFF button which we are used to make ON and OFF light.

the client's request is examined to see if it indicates a button press on the web page. If it does, the state of the GPIO is changed according to the request. If the request indicates "ON", the pin is turned HIGH and the state variable isupdated accordingly and users will be allowed to perform this all activity remotely that is the benefit of the system. Thissystem will work efficiently if no no third person comes into the picture but we all know how popular cyber attacks are these days! That's why we are actually implementing the security mechanismto the system. For that we have takenanotherNode MCU which will keep watch on the malicious activity on the automation system side as well as server side. And if such things happened it will block the attacker and automatically configure the device and the user will let themknow that the systemwas hacked and then whatever the new authentication information will get set by the user, and that attacker will permanently get blocked once its IP address gets tracedbythe system. Now the systemis completely secure and attack free. In this way our system performs its functionality.

Result of Implementation

Fig 1.2

Fig 1.3

Fig 1.4

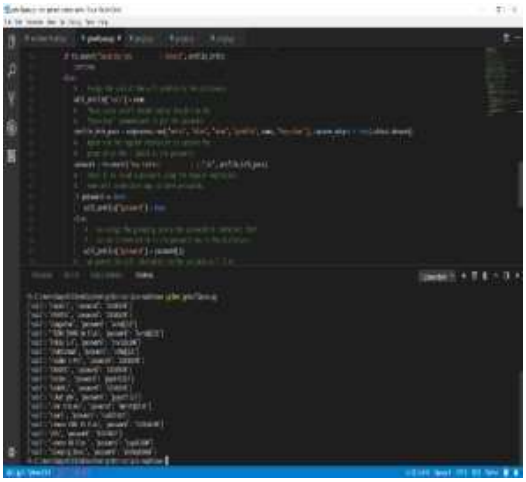

Fig 1.5

4. CONCLUSION

In this project we are going to discuss IoT applications along with

the protocols which it uses for communicating withother smart devices. IoT Smart application is susceptible to various types of attacks. In order to have a secure IoT application. Threat Modelling is used to improve the state of security of Smart application. We focused on Smart Light Bulb application. With threat modeling on Smart Bulb, we noticed some shortcomings with protocols such as Bluetoothinterms of security. An efficient and secure IDS we are goingtousefor securing individual IoT devices.

5. REFERENCES

[1] M. lab, "Csaw esc 2018 github," 2018.[Online] .Available:https://github.com/momalab/csawesc 2019

[2] E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, pp. 3–12.

[3] A. S. Eyal Ronen, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights - IEEE Conference Publication." [Online]. Available: https://ieeexplore.ieee.org/document/7467343

[4] (2017) Zigbee over-the-air upgrading cluster version 1.1 - zigbee document 095264r23.

[5] Securing Smart Home: Technologies, Security Challenges, and Security Requirements

[6] IoT: Security Challenges and Issues of Smart Homes/Cities

