https://dx.doi.org/10.22161/ijaers.6.1.3 ISSN: 2349-6495(P) | 2456-1908(O)

An Experiment with DDoS Attack on NodeMCU12e Devices for IoT with T50 Kali Linux

Antonio Carlos Bento[1], Ellen Martins Lopes da Silva[2], Marcelo Galdino[3], José Carmino Gomes Júnior[4]

[1]Computing Dept., Universidade Nove de Julho, Brazil
Email: acb01@hotmail.com
[2]Computing Dept., Universidade Nove de Julho, Brazil
Email: ellenmmartins@yahoo.com.br
[3]Computing Dept., Universidade Nove de Julho, Brazil
Email: gmgaldino@uni9.pro.br
[4]Computing Dept., Universidade Nove de Julho, Brazil
Email: mat.jose.carmino@gmail.com

***Abstract*—** *This paper presents the results of an experiment with the Kali Linux operating system and T50 tool to simulate Distributed Denial of Service (DDoS) attacks on the NodeMCU12e controller device used in Internet of Things (IoT) projects. The motivation for the development of this study arose with the creation of different projects that deal with the subject involving the Internet of Things, as a necessity to evaluate the safety and capacity of these devices during an attack simulation, which affects security and exposes the fragility of architecture and construction model. The results showed the types of attacks that can be carried out, as well as the device's lack of ability to avoid these types of attacks, as well as the speed at which it is possible to stop the device services.*

Keywords—security; IoT; NodeMCU12e; T50; Kali Linux; DDos.

I. INTRODUCTION

The projects involving the Internet of Things stand out in the national and international market, mainly for the ease of connection between the different types of devices and equipment, allowing the creation of different types of projects that can meet the most varied needs, low cost and the experience of creating solutions quickly, yet with the ease of remote communication, provide an innovative and flexible experience.

When faced with academic research projects that use the Internet of Things as an object of study, it was possible to perceive the great possibilities of applications that this new technology provides, in this way several experiments were carried out with updated models to control equipment monitoring, or even to keep track of the health of individuals. The question that surrounds this study is a security analysis related to the access and use of the Internetof Things devices, which are usually interconnected by some type of network.

The Internet of Things as explained by CERP [8] and ITU-T [12], is a new technology that allows communication between things such as objects, devices or even equations can somehow communicate with one another, this by the ease of communication between a local network, internet type, radio and others. Evolving in conjunction with automation and mechatronics, the Internet of Things is an inexpensive and easily accessible technology, enabling the creation of the most varied solutions.

Due to the fact that it is an emerging technology, it lacks scientific content that can collaborate with the development and serve as a study base for new projects, in this way this work proposes to present the rest of an experiment that involves the security of the normally used disasitives in projects for the Internet of Things, and can serve as a theoretical basis for the creation of new solutions.

Security studies are also a great challenge because the possibilities and types of attacks can in some way stop several types of services or even damage equipment of different types of applications, so this study provides a type of simulation that may allow the researcher to apply in their projects, to somehow study the types of attacks that the devices may suffer during their use, also considering the impacts they may cause.

https://dx.doi.org/10.22161/ijaers.6.1.3 ISSN: 2349-6495(P) | 2456-1908(O)

Several projects on residential, business or even service monitoring are presented, as well as applications directed to the health area, all of which may be impacted by some kind of invasion or security attack. strategies and techniques of prevention, with the most known types of attacks, in this study as a restriction of the project, only some types of attacks should be analyzed, these being the best known, proposed solutions may be presented in future studies, due to their extension and complexity.

The experiments were performed on a specific type of device, such as a controller, this device is usually used in conjunction with other devices, or even sensors, such as temperature, heart rate, pulse or devices as Arduino Uno, the most common, with little capacity, being used for small prototypes, or even for projects where a large operating process is not necessary and with very advanced controls.

With the rapid creation of devices provided to meet the different needs of the market, this project intends to attend a moment in which the concepts of INternet of Things are still in evolution, on the most varied processes, thus allowing a reflection on the need to to devote greater attention, also to studies that involve the security of the types of networks and devices used for the Internet of Things.

II. BIBLIOGRAPH REVIEW

When the bibliographic research was carried out on the key words that compose this work, the most relevant bases were used with IEEE Xplore, IEEE Latinamerca, Scopus and Google Scholar, and these did not present relevant results for the keywords IoT and T50, demonstrating that this research has relevant subject to compose the content in these basses of knowledge.

In this way, the scientific work involving general subjects, such as those that deal with the Internet of Things, was used as basic theory, some equivalent devices, as in the case of the Arduino controller, also relating the experience of some authors about the System Operational kali Linux, this being an appropriate environment for conducting simulations involving security.

Due to this lack of scientific references, technical papers and documentation, provided by manufacturers and specialists, were analyzed, as well as code libraries and discussion blogs. The technical documents collaborated with the practical experiment, enabling the tests and configurations, adapting the project to meet its objectives in the creation of a model that allows the simulation of DDoS-type attacks.

The internet of things is the main subject addressed in this study, considering the documents presented by CERP [8] and ITU-T [12], which are organizations responsible for maintaining, defining and releasing the relevant contents with the projects developed for the Internet of Things , being these models that are adopted by specialists in all the world.

The IEEE baselines are also of major importance because they are the main basis for information on academic contents, journals, conferences on subjects that deal with electronics, computing, security, networks and systems, often many important references are found in this base, allowing the distribution of academic and technical knowledge on different subjects and projects that approach the theme.

Most of the results obtained with this study are of practical origin, with the experience obtained in previous projects such as those presented by Bento [7], these experiences were the pillar of support for the realization of the project, incorporating other studies of relevant authors, even of specialists in the area who collaborated with the materials and references.

The bibliographical references on the methodology and techniques used to develop the structure of this article were developed based on the books and documents presented by Bento [7], Lakatos and Marconi [19], being thes last reference on best practices in the structure of project development of national research.

The studies were developed on the subject Internet of Things based on the works presented by: T. Shah ; S. Venkatesan [23]; F. Wu ; C. Rüdiger ; J.-M. Redouté ; M. R. Yuce [11], E. R. Naru ; H. Saini ; M. Sharma [10]. CERP[8], ITU-T[12].

Studies on the NodeMCU12 controller were developed based on: D. Naranjo ; P. Córdova ; C. Gordon [9], A. P. Murdan ; M. Z. A. Emambocus [3], L. K. P. Saputra ; Y. Lukito [14], M. Edward ; K. Karyono ; H. Meidia [18],

Topics that addressed the types of DDoS attacks were based on the documents presented by: L. Liang ; K. Zheng ; Q. Sheng ; X. Huang [15]; V. Visoottiviseth ; P. Akarasiriwong ; S. Chaiyasart ; S. Chotivatunyu [24]; A. H. Dar ; B. Habib ; F. Khurshid ; M. T. Banday [1]; S.P. Kadam ; B. Mahajan ; M. Patanwala ; P. Sanas ; S. Vidyarthi [22]; S. Arkadii ; C. Vadym [21].

Studies on the Kali Linux operating system were performed considering the works presented by: R. Gaddam ; M. Nandhini [20]; M. Denis ; C. Zena ; T. Hayajneh [17]; J. Narayan Goel ; B. M. Mehtre [13]; A. Hussain Dar ; B. Habib ; F. Khurshid ; M. Tariq Banday [1]; M. A. C. Aung ; K. P. Thant [16]; B. Scott ; J. Xu ; J. Zhang ; A. Brown ; E. Clark ; X. Yuan ; A. Yu ; K. Williams. [6].

https://dx.doi.org/10.22161/ijaers.6.1.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

III. METHOD AND MATHERIALS

As a method, an experimental research was used, in which the technical studies developed on the devices are applied, as explained by Lakatos and Marconi [19] the objective of an experimental research is the creation of experiments that may represent some determinate phenomenon for analysis and evaluation purposes of the data collected during the research development.

Some types of research methods such as Lakatos & Marconi [19] and Bento [7], it is possible to verify the different forms of survey and analysis that can be applied in the most varied study models. In this case, this work has as specific objective to present the results according to the experiments developed on technological resources available in the national and international market.

As a first step, research was done on scientific research materials, technical documents and manuals of manufacturers, after the studies carried out, a comparative and practical analysis was developed on the devices to understand their workings, as well as their adequacy with the proposal of the studies, thus taking as its basis its technological resources and applicability.

After the studies were performed with the tools available in the Kali Linux operating system, with the purpose of understanding their application and structure characteristics, in this way it was possible to choose among the various tools available in the operating system, the library was then selected T50 tools, by itself a model with clear documentation and with simplicity for application in different environments.

After the initial understanding and tests, the devices and equipment necessary to apply the hypothesis of creating a possible environment for simulation of the attack tests with the T50 tool available in the Kali Linux Operating System were selected.

As material was used: a NodeMCU12e controller device, this device was selected due to comparative tests performed in the studies presented by Bento [7], highlighting its capacity, speed, size and low cost, incomapration with other controllers available in the market, such as the Arduino Uno.

The NodeMCU12e device was used in isolation during the project, only to meet the DDoS attack tests, because it has a system that allows it to act as a WiFi access point, because it has this recurrence already built into its architecture, in this way it was possible to carry out the attack simulations.

A Samsung 4G smartphone was also used to be used as a Web connection service, thus enabling the smartphone to communicate with two other computers, one notebook running the Kali Linux Operating System and the T50 library, another notebook with the Windows 10 64 operating system bits to connect to the NodeMCU12e controller and access your home page with Mozilla Firefox web browser, verifying that the connection is online and monitoring the resources used in the network.

In this way it was possible to analyze communications and data traffic between the devices, observing the results of the simulated attacks, enabling the creation of reports and the discussion about the data collected during the survey, a miniUSB cable was also used to connect the controller to the notebook and supply the power required to power the device, the Arduino IDE was used for construct the controller Algoritm.

IV. RESULTS AND DISCUSSIONS

In the initial studies, tools were analyzed that allow the simulation of Distributed Denial of Services (DDoS) attacks [1] [2] [6][13], that is, the sending of a large amount of data packet to stop the services of Web page servers, in this case the NodeMCU12e [7] [18], has features that enable it as an access point server, providing access to internal pages as if it were a web server.

A smartphone with external WiFi access was only used to allow external access to a WiFi network, the NodeMCU12e [7] controller can work in both formats, ie as an access provider and a client, and also has the ability to access pages in other external servers, these features can be manually configured in the device algorithm.

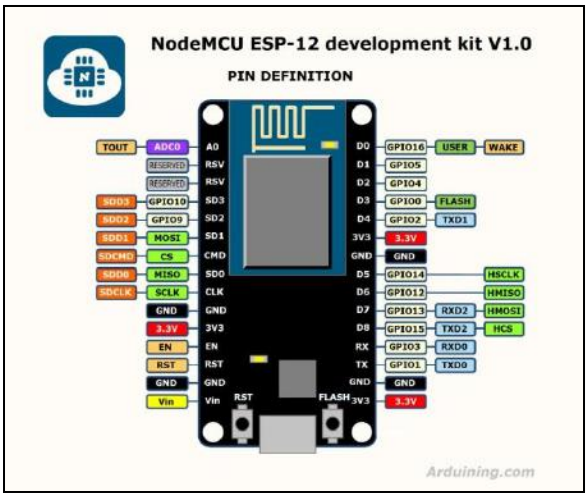

Fig. 1.NodeMCU 12e device connection diagram.

The NodeMCU12e controller device was configured as an access point, using the IP address 192.168.43.39, in this way the computers were used as clients to access the network provided by the device, thus allowing the simulation of the attacks and the monitoring of the services, for analyzing the results and tests, as shown at Fig 2.

Some important characteristics for NodeMCU controller are: CPU 32-bit RISC: Tensilica Xtensa LX106 with 80 MHz; 64 KB RAM memory; 96 KB data; Flash

https://dx.doi.org/10.22161/ijaers.6.1.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

QSPI External - with 512 KB to 4 MB; IEEE 802.11 b / g / n Wi-Fi; 16 pins GPIO; SPI, I2C.

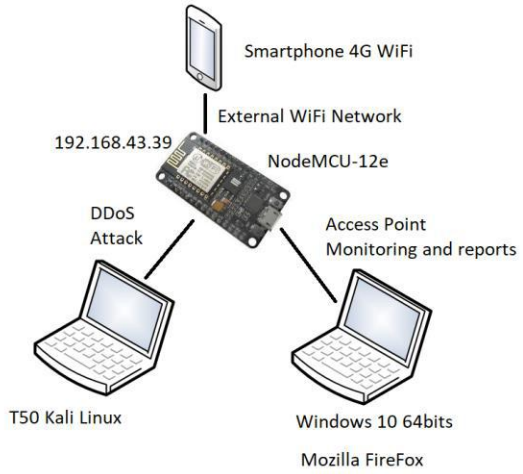

Fig. 2.Network diagram with the devices and connections used during the project.

For the construction of the algorithm, the Arduino IDE, an available tool for the development of algorithms for controller devices, was used, after the proper configuration, downloading of the libraries and access tests, one of the algorithm examples available in the tool, called NodeMCu AdvancedWebServer.ino, available soon after the installation of the correct library of the controlling device.

As an initial part of the configurations, the following libraries were used as well as the settings to access the controller device, it is important to observe the ESP8266WebServer command which allows configuring the device with an access server on port 80, the complete algoritm can be found with the Arduino IDE settings.

```
#include <ESP8266WiFi.h>
#include <WiFiClient.h>
#include <ESP8266WebServer.h>
#include <ESP8266mDNS.h>
const char *ssid = "yourSSID";
const char *password = "YourSSIDPass";
ESP8266WebServer  server ( 80 );
```

Another important point is to observe the *ssid and *password variables, these must be used to access the external WiFi network available on the Smartphone, this feature is used simply for the controller to have client access and on external websites, such a resource should not be used in this project.

The controller algorithm generates a random graph when accessing the address by the web browser, demonstrating its active operation during access, in this way it is possible to monitor the access, the values vary every three seconds, presenting a new graphic, thus it is possible to identify if the access point is operational.

Fig. 3.NodeMCU 12e monitoring screen via WiFi site.

Before the DDoS attack simulation Fig. 3, the network and devices have the following status, observing that there is only one computer with the Kali Linux operating system and another one computer with the Windows operating system on the same network, one to validate the attack and another to monitor the accesses to the controller, to generate the transfer tax reports Fig. 4.

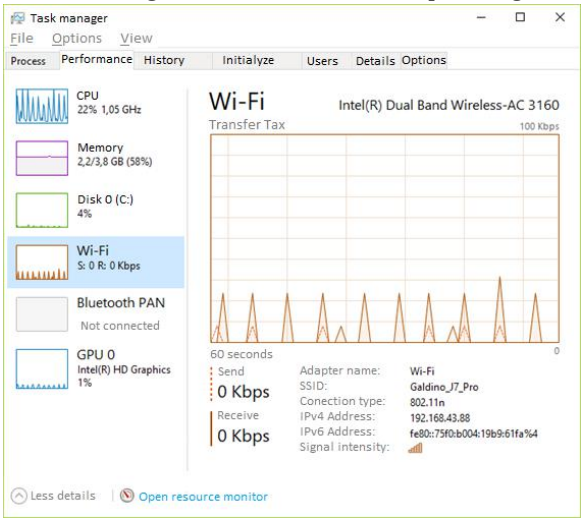

Fig. 4.Task monitor running on the Windows 10 computer for monitoring the network tax transfer.

Fig. 5.

At this moment the constant status of the transmission rate and reception of the network data before the attack simulation is considered, considering an updated analysis every sixty seconds interval, after which the transmission processes for DDoS attack simulation are started Fig. 5.

Denial-of-service attacks are a specific class of pentest attacks (Penetration Testing, in which the idea is to send an excess of packets to a particular server.

Because the device or server is not ready to receive this high packet load, it will be overloaded, this will cause your bandwidth to slow and even crash.

Basic commands used with T50:

```
root@kali:~#  t50 --flood 192.168.43.39
entering in flood mode...
```

https://dx.doi.org/10.22161/ijaers.6.1.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

hit CTRL+C to break.

T50 5.4.1-rc1 successfully launched on Oct. 10th 2018 10:48:51

Was used the follow command with the project for test the NodeMCU12e controller:

root@kali:~# t50 192.168.43.39 --flood -S --turbo --dport 80

Details about the command:

t50 : t50 command

192.168.43.39 : target Web server internet protocol

--flood : replace the threshold

-S : TCP SYN Flag

--turbo : Increase the attack performance

--dport 80 : Port 80 used for the attack

How demonstrated in the figures 5, 6, 7, 8 e 9, was used around six windows running the same T50 application for DDoS test attack with the NodeMCU12e device.

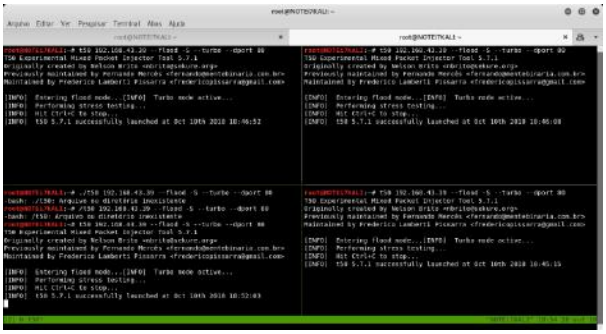

Fig. 6. Four DDoS attack simulation with T50 Kali Linux and packet injection tool 5.7.1.

In that windows fig. 5, is displayed the T50 application in conjunction with another windows.

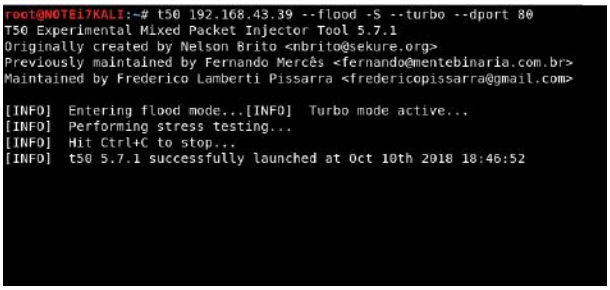

*Fig. 7.*Window 1, packet injection tool 5.7.1.

Fig. 8.

In the fig. 6, is displayed the first command running and sending packages for the device.

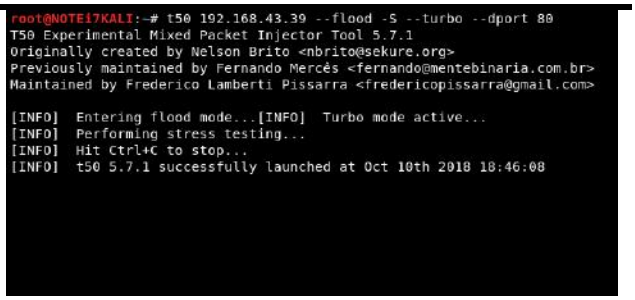

Fig. 9.Window 2, packet injection tool 5.7.1.

Fig. 10.

The same occour with the another windows, where the window 2, 3 and 4 the commands were used in the sequence.

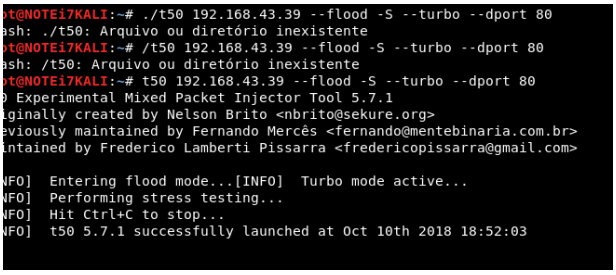

Fig. 11. Windows 3, packet injection tool 5.7.1.

Fig. 12.

With the window 3 fig. 8, is possible verify the DDoS attack in the sequence.

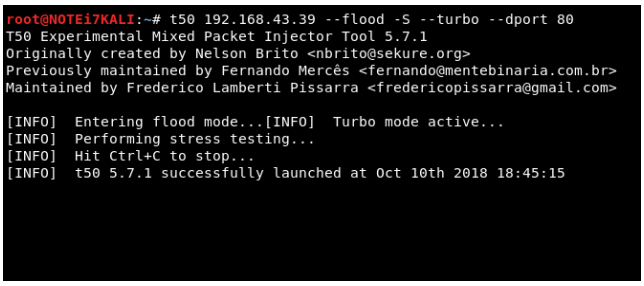

Fig. 13. Windows 4, packet injection tool 5.7.1.

Fig. 14.

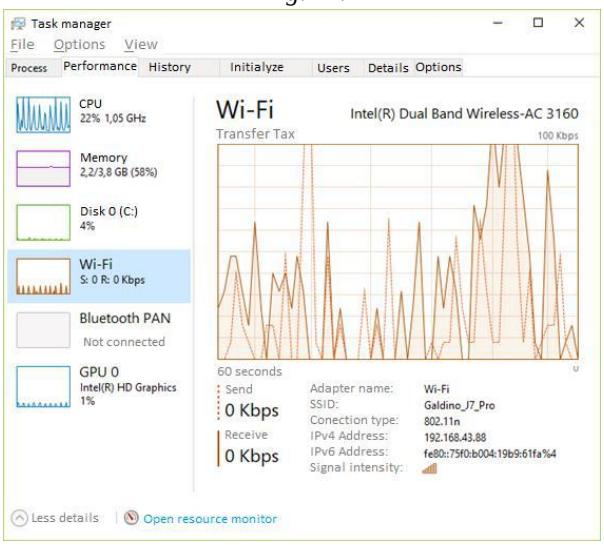

Fig. 15. Results attack after the DDoS simulaton, with the network and NodeMCU12e controller overload.

https://dx.doi.org/10.22161/ijaers.6.1.3 ISSN: 2349-6495(P) | 2456-1908(O)

In the same time another computer was connected with the NodeMCU12e access point address, 192.168.43.39, that computer was used for monitoring the network and to access the NodeMCU12 webserver, monitoring the site access during the attack, the results show the site out of operations during the attack fig 11.

Fig. 16. NodeMCu12e monitoring site not working after the overload test.

Fig. 17.

After the six sequence of commands was possbile to analyze the results, when overloading the device NodeMCU12e with packages of data, this kind of attack is very usual when using address available in the internet, the results has demonstrated the capacity of the device for stay in operation during a usual attack, for only few seconds.

V. CONCLUSIONS

Based on the results obtained, it is possible to conclude that the Internet of Things presents many advantages ahead of the current devices used in clinics and hospitals, and even in the face of the difficulties, the use of Internet of Things in the area of health can bring several benefits to the professionals and institutions, benefits that contribute to an active monitoring, providing greater quality to the patients and ease of control for the doctor.

When analyzing the advantages of the adherence of a project developed with the Internet of Things, the low cost, the ease in the consultation of data for monitoring and in future visits, sharing of the information by several health information bases, objective organization and clear data and information, preventing diagnosis errors, during prescription and in drug interaction.

As disadvantages, one should consider the lack of a technical professional who understands the various interdisciplinary issues involved, for example, it is necessary to understand electronics, computing, networks, database, programming and still understand about the health area and the type of analysis that can be developed.

ACKNOWLEDGMENT

Special thanks for all students, professors, relatives and coleagues which has collaborated with this project development.

REFERENCES

[1] A. H. Dar ; B. Habib ; F. Khurshid ; M. T. Banday. (2016). Experimental analysis of DDoS attack and it's detection in Eucalyptus private cloud platform. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). pp. 1718-1724.

[2] A. Hussain Dar ; B. Habib ; F. Khurshid ; M. Tariq Banday. (2016). Experimental analysis of DDoS attack and it's detection in Eucalyptus private cloud platform. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). pp 1718-1724.

[3] A. P. Murdan ; M. Z. A. Emambocus. (2018). Indoor positioning system simulation for a robot using radio frequency identification. 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA). IEEE Conference. pp 986-991.

[4] Arduino. 2018. Official Available at: https://www.arduino.cc

[5] B. Da ; P. P. Esnault ; S. Hu ; C. Wang. Identity/identifier-enabled networks (IDEAS) for Internet of Things (IoT). 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE Conferences. pp. 412-415.

[6] B. Scott ; J. Xu ; J. Zhang ; A. Brown ; E. Clark ; X. Yuan ; A. Yu ; K. Williams. (2017). An interactive visualization tool for teaching ARP spoofing attack. 2017 IEEE Frontiers in Education Conference (FIE). IEEE Conference. pp. 1-5.

[7] Bento A. C..IoT: NodeMCU 12e X Arduino Uno, Results of an experimental and comparative survey. International Journal of Advance Research in Computer Science and Management Studies, v. 6, p. 46-56, 2018.

[8] CERP. (2009). IoT – Internet of Thinsgs of European Research Cluster. Internet of things: Strategic Reserach Roadmap, Available at: http://www.internet-of-thingsresearch.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

[9] D. Naranjo ; P. Córdova ; C. Gordon. (2018). Wearable Electrocardiograph. 2018 International Conference on eDemocracy & eGovernment (ICEDEG). IEEE Conference. pp 201-205.

[10] E. R. Naru ; H. Saini ; M. Sharma. (2017). A recent review on lightweight cryptography in IoT. 2017 International Conference on I-SMAC (IoT in Social,

https://dx.doi.org/10.22161/ijaers.6.1.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

Mobile, Analytics and Cloud) (I-SMAC). IEEE Conferences. pp. 887-890.

[11] F. Wu ; C. Rüdiger ; J.-M. Redouté ; M. R. Yuce. (2018). W.E-Safe: A wearable IoT sensor node for safety applications via LoRa. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE Conferences. pp 144-148.

[12] ITU-T. (2012). Internet of Things Global Standards Initiative. Available at: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

[13] J. Narayan Goel ; B. M. Mehtre. (2014). Dynamic IPv6 activation based defense for IPv6 router advertisement flooding (DoS) attack. 2014 IEEE International Conference on Computational Intelligence and Computing Research. IEEE COnference. pp 1-5.

[14] L. K. P. Saputra ; Y. Lukito. (2017). Implementation of air conditioning control system using REST protocol based on NodeMCU ESP8266. IEEE Conferences. pp. 126-130.

[15] L. Liang ; K. Zheng ; Q. Sheng ; X. Huang. (2016). A Denial of Service Attack Method for an IoT System. 2016 8th International Conference on Information Technology in Medicine and Education (ITME). IEEE Conferences, pp. 360-364.

[16] M. A. C. Aung ; K. P. Thant. Detection and mitigation of wireless link layer attacks. 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA). IEEE Conference. pp. 173-178.

[17] M. Denis ; C. Zena ; T. Hayajneh. (2016). Penetration testing: Concepts, attack methods, and defense strategies. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). pp. 1-6.

[18] M. Edward ; K. Karyono ; H. Meidia. (2017). Smart fridge design using NodeMCU and home server based on Raspberry Pi 3. 2017 4th International Conference on New Media Studies (CONMEDIA). IEEE COnferences. pp. 148-151.

[19] Marconi, M.; Lakatos, E. (2017). Fundamentos de metodologia científica. 8. ed. São Paulo, Brasil: Ed. Atlas, 2017. pp. 310.

[20] R. Gaddam ; M. Nandhini. (2017). An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment. 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE Conferences. pp. 10-15.

[21] S. Arkadii ; C. Vadym. (2017). Research on impact of router critical system resources on traffic routing process. : 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). IEEE Conference. DOI: 10.1109/AIACT.2017.8020106.

[22] S.P. Kadam ; B. Mahajan ; M. Patanwala ; P. Sanas ; S. Vidyarthi. (2016). Automated Wi-Fi penetration testing. 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). IEE Conferences. pp. 1092-1096.

[23] T. Shah ; S. Venkatesan. (2018). Authentication of IoT Device and IoT Server Using Secure Vaults. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE Conferences. pp. 819-834.

[24] V. Visoottiviseth ; P. Akarasiriwong ; S. Chaiyasart ; S. Chotivatunyu. (2017). PENTOS: Penetration testing tool for Internet of Thing devices. TENCON 2017 - 2017 IEEE Region 10 Conference; pp. 2279-2284.