Implementation And Analysis Of Virtual Network Security Against DOS And DDOS Attack With Hips Snort

1st Ivan Saputra Zebua
School of Electrical Engineering
Telkom University
Bandung, Indonesia
ivanzebua@student.telkomuniversity.ac.id

2nd Nyoman Bogi Aditya Karna
School of Electrical Engineering
Telkom University
Bandung, Indonesia
aditya@telkomuniversity.co.id

3rd Arif Indra Irawan
School of Electrical Engineering
Telkom University
Bandung, Indonesia
arifirawan@telkomuniversity.ac.id

Abstract —Work From Home (WFH) as a result of the covid 19 epidemic drives the advancement of digitalization. Due to a health regulation that forbids them from interacting with one another, people do all of their activities remotely. Therefore, a telecommunications engineer is required to satisfy the client's internet and web server accessibility requirements. To assure the availability of web servers, however, the availability of the internet must be backed by a robust cyber security system. This research aims to learn IDS behavior against SYN and UDP flood attacks at the transport layer. As a result of this research, HIPS Snort is able to drop 96.65% of DoS SYN flood attack packets, 97.92% of DDoS SYN flood attack packets, 95.54 % of DoS UDP flood attack packets, and 95.07 % of DDoS UDP flood attack packets when activated. Thus, snort can prevent against DoS and DDoS attacks.

Keywords— web server, cyber attack, HIPS snort, SYN flood, UDP flood

I. INTRODUCTION

The covid 19 outbreak hastens digitalization. Pandemic covid 19 pushes people to work from home (WFH). Due of health issues, they must communicate online or WFH. To meet the client's internet and web server accessibility needs, a telecommunications engineer is needed. To ensure web server availability, internet connectivity must be accompanied by cyber security. Websites enable online information sharing. Websites have info pages. Customers visit a website's homepage. Clients can visit the website if the web server answers to inquiries. Web servers must be secure to receive and respond to client requests online. CIA stands for confidentiality, integrity, and availability.

Attackers target web server availability. Web server availability attacks include DoS and DDoS. DoS and DDoS attacks can be stopped by routers. DoS and DDoS defense is IPS. IPS is an IDS that blocks suspicious activity. DoS and DDoS can disable services. DoS and DDoS assaults can hurt IT companies. This study examines HIPS Snort's DoS and DDoS server performance.

[1] Used HIPS Snort to test a virtual web server's SYN Flood defenses. 1 PC is used as a server, 1 as a router, 1 as a client, and 4 as an attacker, all virtual using VMware and HIPS Snort on the server side. 4 attackers averaged 2,454,930 packets per minute against Putra (2018). 2.1% (52,304) of attacks and drops were missed [1]. Putra (2018) exclusively analyzes SYN Flood protection. UDP Flood attacks can target web servers. This research improves website uptime testing. This research explores HIPS Snort's ability to prevent web servers from SYN Flood and UDP Flood attacks by constructing a virtual network to simulate DoS and DDoS attacks using TCP and UDP protocols. DoS/DDoS tool: hping3. Snort is installed on the router to recap attack data.

Based on those issues, it’s important to research about the implementation and analysis of virtual network security against DoS and DDoS attack with HIPS Snort. This research can advance cybersecurity and web server availability against DoS and DDoS attacks. This research is also important for learning IDS behavior against SYN and UDP flood assaults at the transport layer. This

helps examine HIPS Snort's transport layer defenses against SYN flood and UDP flood attacks.

II. THEORITICAL REVIEW

A. Web Server

Servers satisfy client requests. Same-server use is possible. Server-connected clients are served. Internet links clients and servers. Web, mail, database, file, DHCP, proxy, FTP, and game servers are servers. Webservers fulfill HTTP and HTTPS client requests. Webservers service browsers. The web server responds to a browser's code with a webpage. Website pages are client-focused. Printers, cameras, and other devices can also access the webserver.

B. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

DoS is a cyberattack that drains a server's resources. The server and client are attacked. DoS attacks block customer assistance. DoS-like cyberattack. DDoS attackers outnumber DoS. Attackers DDoS one network. One attacker uses zombie PCs to DDoS a server. DoS and DDoS attack servers. [2][3][4]. 1&2 illustrate DoS attacks.

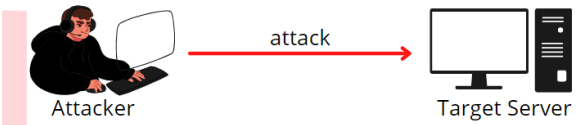

FIGURE 1
DENIAL OF SERVICE (DOS).

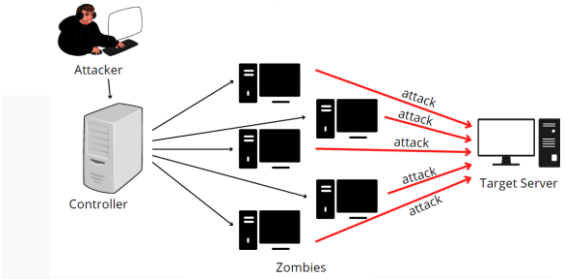

FIGURE 2
DISTRIBUTED DENIAL OF SERVICE (DDOS).

C. SYN Flood Attack

By sending false SYN packets, SYN flood attacks target TCP. The SYN packet begins a "three-way handshake." SYN proposes a new connection from a phony IP address to the destination server. Attacker expects server to process requests [6][7][8][9]. When a server responds a false IP, it waits for a confirmation packet that never arrives, bloating its connection table. The server ignores new connections after the table is filled. Until the attacker quits, legitimate clients can't access the service. DoS and DDoS attacks block real users from a server. DoS and DDoS assaults crash and overwhelm services.

D. UDP Flood Attack

DoS and DDoS attacks using UDP flood are called UDP flood attacks. UDP flooding attacks flood random target ports with UDP packets [10]. UDP is exploitable since it's connectionless, session-less, and lacks internal defenses to control flood rates. Flooding UDP is risky.

E. Snort

Snort is the leading open-source Intrusion Prevention System (IPS) in the world, used to define harmful network activities, locate packets that fit rules, and produce user warnings. Snort's language integrates signature, protocol, and anomaly-based IDS and IPS inspection approaches. Snort employs rules to perform instructions and take action if a package is harmful [5].

III. METHOD

A. System Design

This research is conduct by create a virtual network using the VMware application. The system design to study the behavior of IDS against SYN Flood and UDP Flood attacks at the Transport Layer is explained on this section.

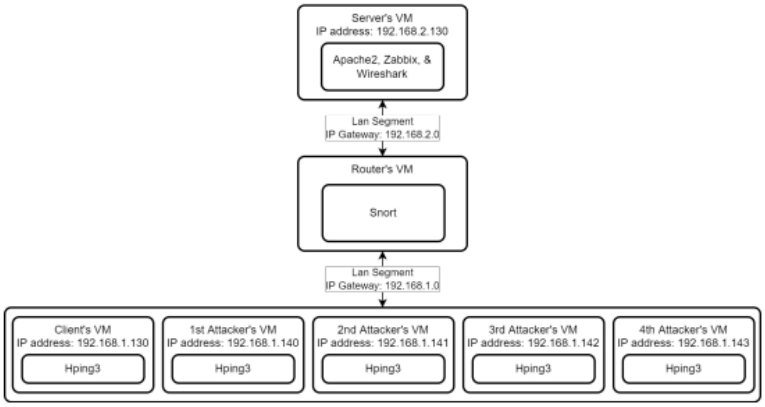

FIGURE 3
SYSTEM DESIGN BLOCK DIAGRAM.

Based on Figure 3.1, this research uses Server, Router, Client, and Attacker VMs. Client and attackers are on the same LAN segment that can interact with the server via router. The system requirements for this research are divided into hardware and software.

1. Hardware
   This research used the following hardware.
   a. A PC with the following spesifications:
      - Processor: AMD Ryzen 7 3750H with Radeon Vega Mobile GFx.
      - 32 Gb RAM.
      - 1 TB HDD.
      - 512 SSD.
   b. A LAN cable with following spesifications:
      - 15 meters cable length.
      - Up to 10 Gbps data transfer speed.
2. Software
   This research used the following software.
   a. Web server's VM with the following spesifications:
      - VM quad-core processor.
      - 8 Gb RAM.
      - 20 Gb ROM.
      - 2 network adapters.
      - Apache 2.
      - Zabbix.
      - Wireshark.
   b. Router's VM with the following spesifications:
      - VM dual-core processor.
      - 2 Gb RAM.
      - 20 Gb ROM.
      - 3 network adapters.
      - Snort.
   c. VM of client and attackers with the following spesifications:
      - VM dual-core processor
      - 2 Gb RAM.
      - 20 Gb ROM.
      - 2 network adapters.
      - Hping3.
      - Wireshark.

B. Research Scenario

This research includes 3 research scenarios based on its parameters. This research tests incoming packets, Snort, and network traffic.

1. Testing the total incoming packets
   This parameter compares the size of incoming packets over a period of time. Systematics for testing total incoming packages:
   a. Examine the client connection percentage before attacked within one minute and tested 40 times.
   b. Examine the client connection percentage since DoS SYN, DDoS SYN, DoS UDP, and DDoS UDP Flood attack within one minute when Snort is non activated and tested 40 times for each attack form.
   c. Examine the number of packets delivered within one minute by one attacker using the SYN Flood attack technique 40 times when Snort is non activated.
   d. Examine the number of packets delivered within one minute by four attackers using the SYN Flood attack technique 40 times when Snort is non activated.

e. Examine the number of packets delivered within one minute by one attacker using the UDP Flood attack technique 40 times when Snort is non activated.
f. Examine the number of packets delivered within one minute by four attackers using the UDP Flood attack technique 40 times when Snort is non activated.

2. Testing using snort
   a. Examine the client connection percentage since DoS SYN, DDoS SYN, DoS UDP, and DDoS UDP attack within one minute when Snort is activated and tested 40 times for each attack form.
   b. Examine the number of packets delivered within one minute by one attacker using the SYN Flood attack technique 40 times when Snort activated.
   c. Examine the number of packets delivered within one minute by four attackers using the SYN Flood attack technique 40 times when Snort activated.
   d. Examine the number of packets delivered within one minute by one attacker using the UDP Flood attack technique 40 times when Snort activated.
   e. Examine the number of packets delivered within one minute by four attackers using the UDP Flood attack technique 40 times when Snort activated.
3. Testing network traffic
   a. Examine the network traffic delivered within one minute by one attacker using the DoS SYN, DDoS SYN, DoS UDP, and DDoS UDP Flood attack technique 40 times when Snort non activated.
   b. Examine the network traffic delivered within one minute by one attacker using the DoS SYN, DDoS SYN, DoS UDP, and DDoS UDP Flood attack technique 40 times when Snort activated.

IV. RESULTS AND DISCUSSION

This part observes and explains the connection between the client and the web server as well as the total number of incoming packets from the attackers. After Snort is deployed to protect the Web server from DoS and DDoS attacks, those data are required to compare with the simulation data.

A. Testing The Total Incoming Packets

Hping3 is used in the test to ping the web server, and an HTTP request is made to check the connection between the client and the web server. In each try, this exam is administered 40 times for a total of one minute.

TABLE 1
CONNECTION BETWEEN CLIENT AND WEB SERVER BEFORE ATTACKED

Attempt	Hping3	HTTP Request		Attempt	Hping3	HTTP Request
1	Success	Success		21	Success	Success
2	Success	Success		22	Success	Success
3	Success	Success		23	Success	Success
4	Success	Success		24	Success	Success
5	Success	Success		25	Success	Success
6	Success	Success		26	Success	Success
7	Success	Success		27	Success	Success
8	Success	Success		28	Success	Success
9	Success	Success		29	Success	Success
10	Success	Success		30	Success	Success
11	Success	Success		31	Success	Success
12	Success	Success		32	Success	Success
13	Success	Success		33	Success	Success
14	Success	Success		34	Success	Success
15	Success	Success		35	Success	Success
16	Success	Success		36	Success	Success
17	Success	Success		37	Success	Success
18	Success	Success		38	Success	Success
19	Success	Success		39	Success	Success
20	Success	Success		40	Success	Success

Table 1 shows that client and web server connections were successful before assault. This subsection compares the client-web server connection during DoS and DDoS assaults to before the attack. The test is divided into four scenarios, including DoS SYN Flood, DoS UDP Flood, DDoS SYN Flood, and DDoS UDP Flood attacks. Each minute-long attempt includes 40 tests. DDoS uses four attackers while DoS only uses one.

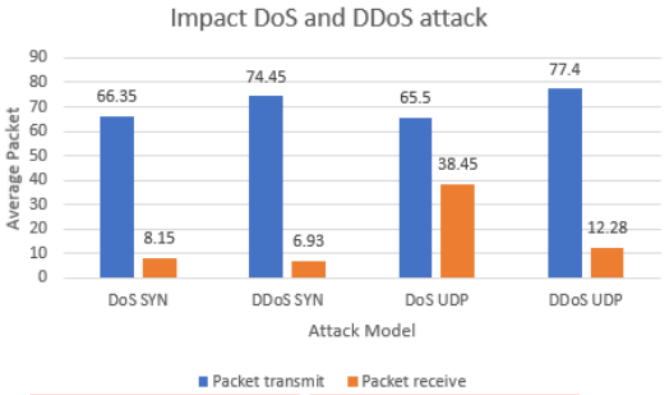

FIGURE 4
IMPACT DOS AND DDOS ATTACK TO CLIENT CONNECTION

Figure 4 depicts how SYN and UDP Flood DoS and DDoS attacks destroy client-server connections. DoS and DDoS attacks prevent web servers from processing client requests. Web servers can send clients 8.15 DoS SYN Flood packets, 6.93 DDoS SYN Flood packets, 38.45 DoS UDP Flood packets, and 12.28 DoS UDP Flood packets. This checks attacker packets. Attackers' web server packet count is tested. 40 times per minute were tried. DoS SYN, DoS UDP, DDoS SYN, DDoS UDP are tested. DDoS uses four attackers, DoS one.

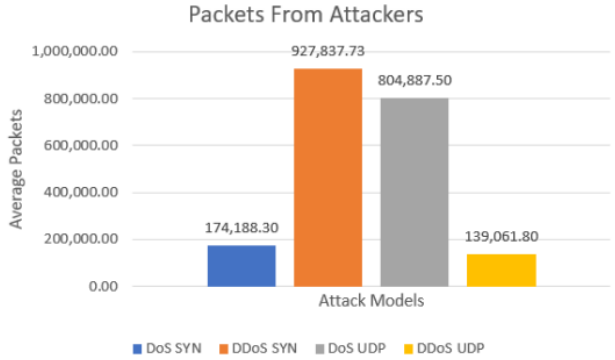

FIGURE 5
AVERAGE PACKETS FROM ATTACKERS

Figure 5 shows attack packets. DDoS SYN Flood creates 927,837.73 packets each attempt. Each DDoS UDP Flood attack uses 139,061.80 packets. Due to a packet collision during the test, attackers send fewer DDoS UDP Flood packets.

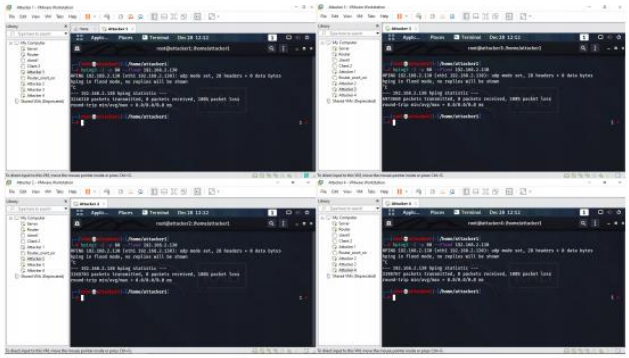

FIGURE 6
SNORT RESULT FOR DDOS UDP COLLISION PACKETS EVIDENCE

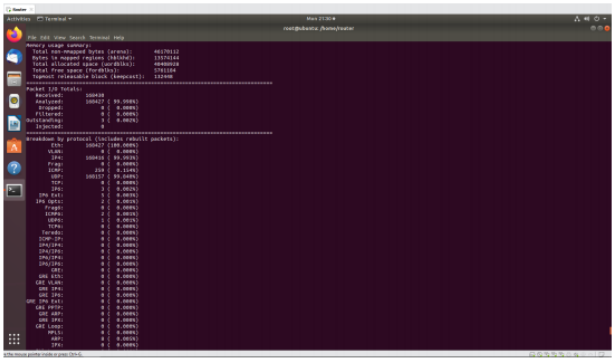

FIGURE 7
SNORT RESULT FOR DDOS UDP COLLISION PACKETS EVIDENCE

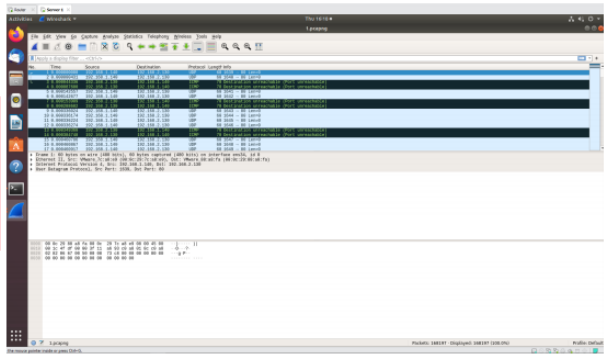

FIGURE 8
SNORT RESULT FOR DDOS UDP COLLISION PACKETS EVIDENCE

The collision packet during a DDoS UDP Flood attack is explained in Figures 6, 7, and 8. The quantity of packets that each attacker transmits is displayed in Figure 6. Attacker packets collide as they go through the air. Figures 7 and 8, which show the total number of incoming packets on the router and the network of the web server, can be used to demonstrate this.

B. Testing Using Snort

This part observes and explains the connection between the client and the web server as well as the overall attack packet drop. To compare such statistics with those from section 4.1, it is necessary. This section is test the client connection when Snort activate and total packet dropped by HIPS Snort.

The test client connection when Snort activate aiming to determine the total amount of client traffic that can reach the web server. Understanding Snort's ability to confirm a successful connection between a client and a web server is useful. This test was run 40 times in each try for a duration of one minute utilizing virtual machines for a web server, router, client, and attacker. Four test scenarios—DoS SYN flood attack, DoS UDP flood attack, DDoS SYN flood attack, and DDoS UDP flood attack—are used in the testing. Whereas a DDoS assault uses four attackers and a DoS attack just uses one.

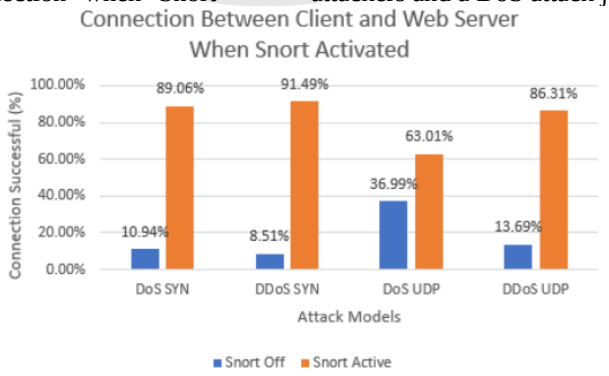

FIGURE 9
CLIENT CONNECTION WHEN SNORT ACTIVE

Figure 9 shows that Snort improves web server-client connections. Snort drops hostile packets so the web server can react to client requests. Snort activated the successful

connection between client and web server during DoS SYN previously 10.94% to 89.06%, DDoS SYN previously 8.51% to 91.49%, DoS UDP previously 36.99% to 63.01%, and DDoS UDP previously 13.69% to 86.31. HIPS Snort's packet-dropping ability is tested. Using web server, router, and attacker VMs, this test is run 40 times in 1 minute. Testing includes DoS SYN Flood, DoS UDP Flood, DDoS SYN Flood, and DDoS UDP Flood. DoS uses 1 attacker and DDoS uses 4 attackers.

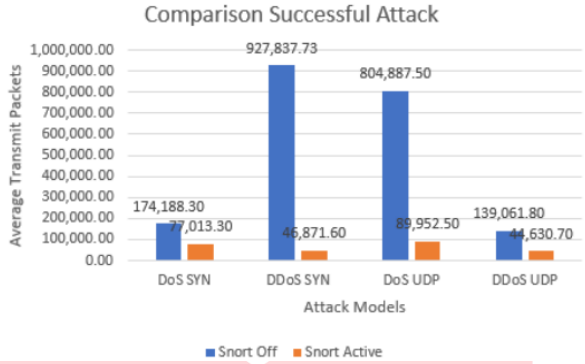

FIGURE 10
TOTAL PACKET DROPPED BY HIPS SNORT

Based on Figure 7 and Table 3, HIPS Snort can prevent web server by dropping SYN and UDP Flood attacks packet with an average 95% above.

C. Testing Network Traffic

This section compares network traffic before and after Snort is activated during DoS and DDoS attacks. DoS and DDoS attacks can exhaust web server resources, so this test compares bandwidth usage during an attack with usage when snort is active. The test is run 40 times in each try for 1 minute utilizing web server, router, client, and attacker VMs. This test includes DoS SYN, DDoS SYN, DoS UDP, and DDoS UDP Flood. Figure 11 shows the test result.

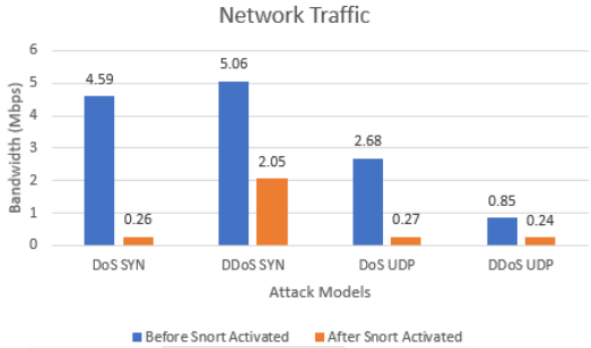

FIGURE 11
COMPARISON NETWORK TRAFFIC DURING TEST

Based on Figure 4.9, Snort reduces network traffic before DoS and DDoS attacks may consume all web server resources by dropping attacker's packets to minimize bandwidth.

V. CONCLUSION

Based on the research in 'Implementation and Analysis of Virtual Network Security Against DoS and DDoS Attack with HIPS Snort,' can be conclude as following:

A. HIPS Snort rules can prevent the web server from SYN Flood and UDP Flood attacks.
B. In a 1 minute simulation, the average packets from an attacker with DoS SYN, DDoS SYN, DoS UDP, and DDoS UDP are 174188.30, 927837.73, 804887.50, and 139061. 80 packets can disrupt the connection between a client and web server, resulting in packet drops of 95.85% during a DoS SYN Flood attack, 99.59% during a DDoS SYN Flood attack, 79.51 during a DoS UDP Flood attack, and 91.45% during a DDoS UDP Flood attack.
C. By using HIPS Snort's rules. It can thwart DoS SYN Flood, DDoS SYN Flood, DoS UDP Flood, and DDoS UDP Flood attacks in 1 minute by dropping 96.65%, 97.92%, 95.547%, and 95.07% assaulting packets. HIPS Snort improves client-web server connectivity.

Where packets drop on client connection during DoS and DDoS attacks are reduced from 96.65% during DoS SYN Flood attack, 97.92% during DDoS SYN Flood attack, 95.54 during DoS UDP Flood attack, and 95.07 during DDoS UDP Flood attack to 89.06% during DoS SYN Flood attack, 91.49 during DDoS SYN Flood attack, 63.01% during DoS UDP Flood attack.

REFERENCES

[1] R.S. Putra, "Implementation and Analysis Virtual Network Security Againsts DoS and DDoS Attack with HIPS Snort," Bandung, 2018, in Indonesian Language.

[2] B. M. C. Y. N. P. Nuno M. GARCIA, FÁBIO GILL and R. I. GOLEVA, "Keyed User Datagram Protocol: Concepts and Operation of An Almost Reliable Connectionless Transport Protocol," IEEE Access, 2019.

[3] P. Lall, "Ransomware and DDoS is On The Rise: Tips for Distance Learning in 2021," McAfee Labs, January 2021

[4] B. S. dan Sandi Negara (BSSN), "Rekap serangan siber (Januari – April 2020)," BSSN.go.id, 2020, in Indonesian Langguage

[5] Rizky, "Implementation and analysis virtual network security against dos and ddos attack with hips snort," Bandung, 2017, in Indonesian Language.

[6] R. Gaddam and D. M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks," IEEE, 2017.

[7] W. H. Maham Qayyum and M. A. Shah, "Performance analysis of snort using network function virtualization," IEEE, 2019.

[8] M. Ankita Sharma and D. A. Bhasin, "Critical investigation of denial of service and distributed denial of service models and tools," IEEE, 2018.

[9] P. D. M. G. D. D. A. A. F. A. R. A. A. H. Maslina Daud, Prof. Dr. Rajah Rasiah "Denial of service: (dos) impact on sensors," IEEE, 2018.

[10] M. M. Kamaldeep and M. Dutta, "Contiki-based mitigation of udp flooding attacks in the internet of things," IEEE, Desember 2017.