Original Research Paper | Computer Science | Volume : 5 ¦ Issue : 12 ¦ Dec 2020 ¦ e-ISSN : 2456-5040

A THREE LAYER SECURITY APPROACH USING HONEYPOT TO MITIGATE DDOS ATTACK IN CLOUD-IOT ECOSYSYTEM

Md Mehedi Hasan[1], Md Hasibul Hassan[2]

[1]Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka-1207, Bangladesh.
[2]Department of computer science and engineering, Ahsanullah University of Science and Technology, Dhaka-1207, Bangladesh.

ABSTRACT

With an increasing number of security threats, various measures have been taken to prevent those malicious events from happening furthermore. Several security risks in the Internet of Things (IoT) have been identified, assessed, and addressed as well. However, yet we are unable to prevent the distributed denial of service (DDoS) attacks on this aspect that, in turn, may hamper the production or other smart features built on top of IoT. Internet of Thing is a network paradigm which connects things (e.g., Smart Phones, Smart TV, Home Appliance, Cars, etc.) to the Internet. Therefore, in this paper, we present three-layer approach utilizing honey pot and demilitarized zone rules to mitigate the devastating consequences caused by DDoS in the cloud-IoT ecosystem. We have developed a framework and rule-based system to protect the internal/external network. In addition, the system can evaluate better outcome by enforcing modified rules in layers in case of DDoS attack. The simulation result, along with the packet analysis, reveals that the layering of rule-based systems shows better result as we are only able to mitigate the threat.

KEYWORDS: IoT security, honey pot, DDoS attack, cloud.

I. INTRODUCTION:

The Internet of things (IoT) is a network of distributed(sensor) nodes, (cloud) servers, and software. This paradigm permits measurements to be sensed and processed in real-time creating a direct interaction platform between cyber-physical systems. Such an approach results in improved efficiency within the generation and usage of knowledge resulting in economic benefits [1]. Internet of Things (IoT) is the next era in the IT world that would take the technology to new heights. IoT takes the Internet from its infancy and transforms it into a fully integrated form of the Internet. As the Internet revolutionized the connectivity of people, similarly IoT will change the world into a smarter world where objects would communicate with others.[2] Cloud computing has emerged as a popular computing model to support the processing of volumetric data using clusters of commodity computers. Nowadays, the computational world is choosing pay-for-use models. Hype and discussion aside, there remains no concrete definition of cloud computing [3].

Denial-of-Service (DoS) attack is a type of attack which is used to temporarily or indefinitely shut down the system/network, thus disallowing the intended users to access it. It is achieved by pinging the system with a load of spam requests which the system won't be able to handle i.e., the system's processing power will be limited and loading it with a lot of spam requests will tend to overload and crash it. It is achieved through various methods, the most famous of them being botnets and buffer overflow vulnerability [4]A denial of service attack results in a temporary or long-term non-availability of service to its intended users by way of either crashing a service resulting in complete non-availability or by flooding a server with fraudulent requests thereby slowing down the delivery of service to real users [5].

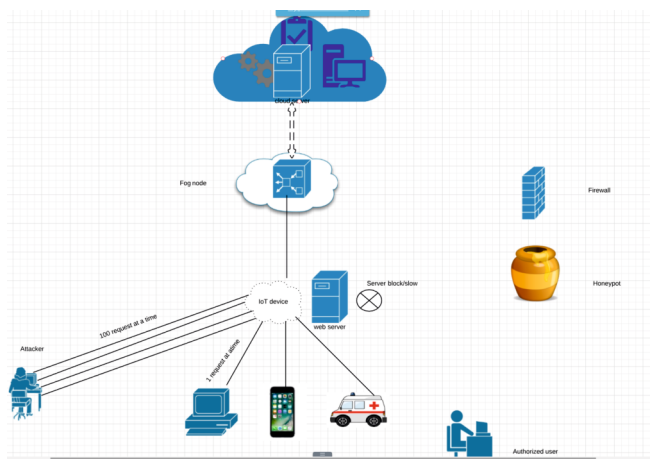

Fig 1: Block diagram of DDoS attack

Honeypots are proposed to act as traps for malicious attackers. However, because of their deployment at fixed (thus detectable) locations and on machines other than the ones they are supposed to protect, honeypots can be avoided by sophisticated attacks [6]. Honeypots are proposed to act as traps for malicious attackers. However, because of their deployment at fixed (thus detectable) locations and on machines other than the ones they are supposed to protect, honeypots can be avoided by sophisticated attacks [6].

Honeypot is a system that is used to mimic the main system by luring potential hackers who seek to gain unauthorized access to information systems. It is used to study activities traces left by hackers and to rectify the system's securities in order to prevent future attacks. Generally, it consists of a computer, applications, and data that simulate the behavior and acts as a decoy. It is usually a part of the firewall so that it can be controlled easily. Based on the design and deployment, honeypots are classified as either production or research honeypots.

Research honeypots are run to have a detailed study about the intruder and safety security measures while production honeypots are placed in a production network to serve the role of a decoy as part of the intrusion detection system [7]. Honeypots are physical or virtual machines successfully used as intrusion detection tools to detect worm-infected hosts. Denial of service (DoS) the attack consumes the resources of a remote client or the network itself, thereby denying or degrading the service to the legitimate users [8] Cloud Computing may be a jargon, in other words, a new computing model, in which the public Internet is used to connect to the provider's hosted network, Infrastructure, platform, and applications to leverage reliable services. Cloud has left all other distributed computing structures/mechanisms far behind both in competition and terms of popularity and success [9]. The primary reason is that any service are often scaled up or down as and when required, supported customer's needs. Cloud offers flexibility [10].essentially a combination of existing technologies that are to succeeding in making a paradigm shift in building and maintaining distributed computing systems making use of multiprocessor, virtualization technology, network-based distributed data storage, and networking. The cloud providers have Infrastructure as a Service (IaaS) [11], Platform as a Service (PaaS), and Software as a Service (SaaS) and lots of more services to supply

II. RELATED WORK:

IoT may be a network of distributed (sensor) nodes, (cloud) servers, and software. This paradigm permits measurements to be sensed and processed in real-time creating a direct interaction platform between cyber-physical systems. Such an approach leads to improved efficiency in the generation and usage of data leading to economic benefits [1] The mechanism works in two steps: First, they can defend their operational network with a high probability against known DDoS and new, future variants. Second, they trap the attacker so that recording of the compromise can help in legal action against the attacker [9]

In the proposed model, the system works in two states as depicted in the two method Primary Scenario and Secondary Scenario they can simulate results as an increase of 55 to 60 in efficiency when a honeypot is implemented But In this works would not be to collect and analyze outcomes for the proposed model implemented in a real-time environment which is not capable of handling, since the verification system for this model might prove incapable there [3].

This author [9] approaches can be categorized into two broad categories: mitigation of the impact/detection of the attack and identification of the source of the attack. The first group includes measures as (a) filtering packets, (b) disabling broadcasts and unused services, and (c) applying security patches. The second area of proposals focuses on identifying the source of the DoS attack.

The author has analyzed the existing honeypot system to identify some of the problems, such as the Legitimate Attacker and Link Unreachable problem. The Legitimate Attacker problem is solved by opening a virtual or physical communication port. But the problem is that If one or more unauthorized clients is sending wrong Auth-Req to dedicated or not dedicated to a client, it will cause an interrupt [11].

With regard to DoS attacks on IoT, we would like to highlight the research was undertaken and the ideas proposed to deal with this disastrous attack. Sudip Misra et al. [4] suggests learning automata-based approach to deal with DDoS attacks in IoT systems.

The primary objective of this work with sub issues as follows:

- To Identify the problem as well as in mitigate DDoS attack To Establish framework and rule based system to protect internal/external network
- To Develop a DDoS attack mitigate architecture
- To Secure network affected by DDoS attack
- To Identify attacker and initiative reduce DDoS attack

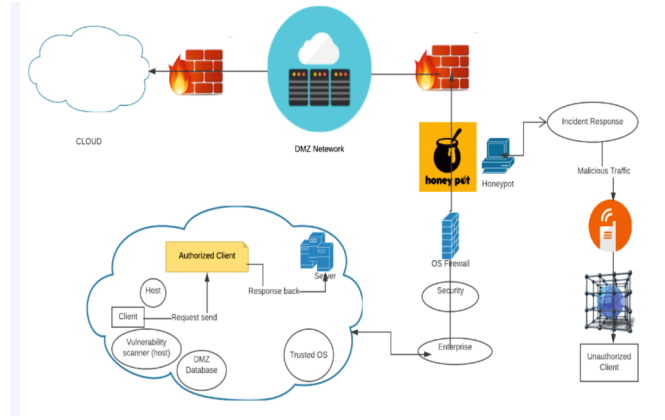

Fig 2: System model

The rest of the paper is organized as follows: Section II presents detailed literature review on security prospects in IoT with analyzing scopes and limitations. Section III discusses the overall methodology of our proposed multi-tier security system with providing necessary flow diagrams. Then Section IV proves the validity of our proposed base. Finally, Section V looks into the applications, scopes, limitations and future directions of the work before coming to a conclusion.

III. METHODOLOGY:

Considering DDos attack, We are analysis and find more rules and more secure methodology according to previous work and studies on mitigating about dos attack in Honeypot. And our target basically set a better approach to build a high-efficiency rate based on previous work so we are working 3 layered architecture.

- First, create honeypot act like intrusion detection/intrusion prevention system.
- Second, create a database for honeypot which traffic enters decide by honeypot rules
- Third, create a DMZ network for external user

A. Allowing real traffic:

As we can see our expectation our internal network system and external network use frequently and easily clients are satisfied our system So, we are trying to only enter real traffic in our system malicious traffic always avoid this framework it is the target if rule works well.

B. Blocking malicious traffic by using Honeypot:

If someone tries to entry to our system as well as unauthorized, honeypot identify as malicious traffic so honeypot block it bypasses according to rules.

C. Rules set:

We using KFsensor to detect malicious traffic, basically Kfsensor is an intrusion detection system also it can be work as well as intrusion prevention system. here we create a rule for how many traffic enters our system or access our system we can define in the Kfsensor.

- We are trying to see and analysis UDP packet flooding how many UDP packets is real and malicious. So we are rules set like only max connection per IP 20 and max concurrent per IP 15.
- We are trying to see and analysis TCP packet flooding how many TCP packets is real and malicious. So we are rules set like only max connection per IP 20 and max concurrent per IP 15

D. Create Demilitarized Zone Network:

At this part, we create demilitarized zone for external users basically, in this networking use for a specific server or special IP who decide by the rules system overall decision can making by which is monitoring an internal and external network, if all rules work according to architecture Figure:3 And another work in demilitarized zone part is that if an external user or IP address requests to the server then rules match and demilitarized zone network referred to the server which is defined by the system which one using by external all are showed.

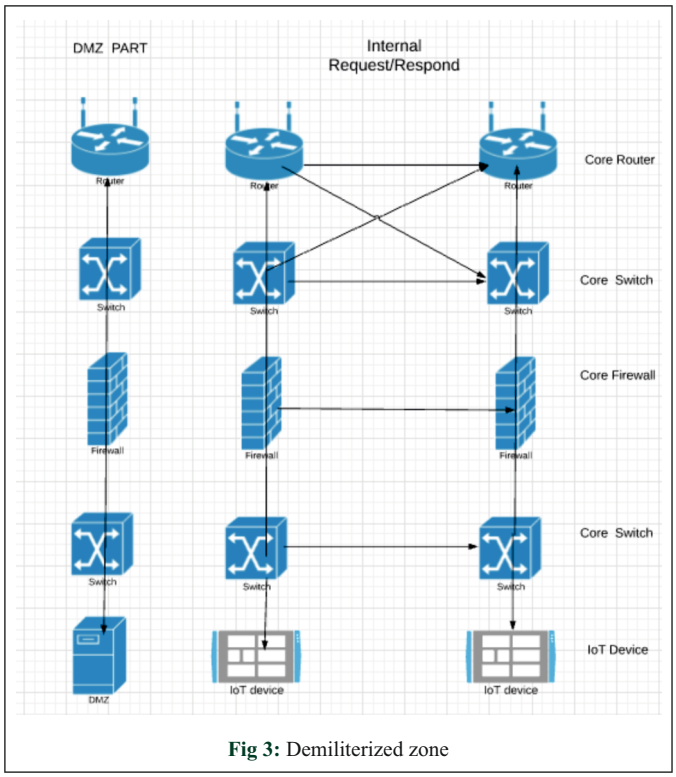

Fig 3: Demiliterized zone

E. Create Firewall:

At this part, we create a firewall for external users or internal basically, in this section work as a gate a man in which traffic enters the system and which traffic going outside decide by the system according to rules and methods

F. Algorithm:

Algorithms of Detect malicious traffic,according to rules, and algorithm two are mitigate dos attack.

Algorithm 1 for access ineternal server

```
Input     :   If Internal user request
Output    :   Access Internal serve
System Initialization;
Receive data packet from internal user ;
If DMZFirewall_Honeypot_Rulesmatch and
   Clientrequest=5=True  then
     Set GotInternalserver
       While  Request receive do
          Take packet in a certain range;
          Create array for input data set;
        For Rangeeach  do
          Request IP adress,MAC address,Port must be
          Match after permission to access internal S;
             While Accesstoserver S;
```

Cheek Honeypot rule if match give
Permission to access Is;
End
Send Packet to Honeypot;cheek Rule;
Then get permission to access;
End
End
End
Discards Request
End

IV. IMPLEMENTATION AND RESULTS:

A. Hardware components:

In this work, we use the Cisco router for based on rule cheek and established connectivity between enterprise network to observe malicious traffic and real traffic analysis. based on this paper we used an operating system such as Windows PC and Linux PC to collect data and analysis via wire shark.

B. Software components:

In this part using several software at first we using a Kfsensor (2.0.1) It is honeypot tools act like intrusion detection system and intrusion prevention system. then we use a for creating Dos attack low orbit Ion Canon(1.0.8), and My SQL it is open source we use this for creating a database, and last of wire shark(3.2.2) for packet capturing.

C. Results and perfomance:

As far as we know DDoS attacks cannot prevent but it can be mitigated and we try to reduce the rate. if this work follow and maintain all the rules and the system can work it results we can see in figure 4 and 5 when malicious traffic entering the system the wave high and when our system get permission to entering authorized or rule-based IP which we declared and save onto the database it is act normally. And we create a DMZ network for using the external user as well as set a firewall rule for minimum traffic entering a system.

So, this work is rule based on every stage of the system. if we need to extend to entering IP on our system we just change its rule and work frequently.

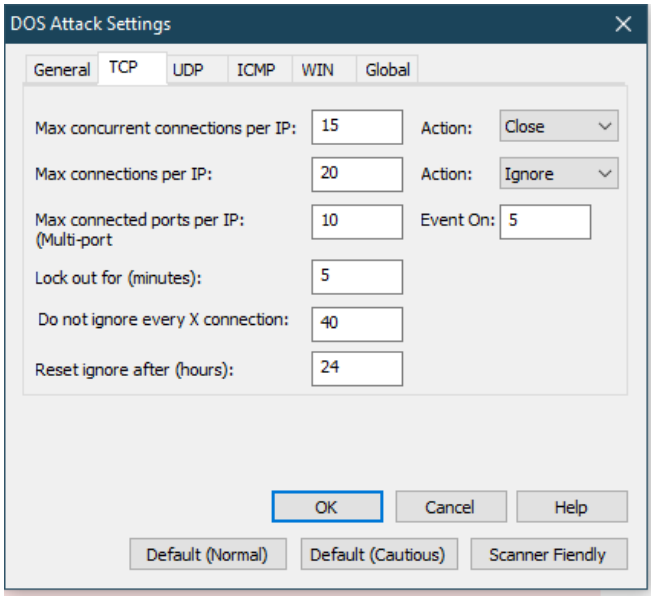

Fig 4: TCP rule set.

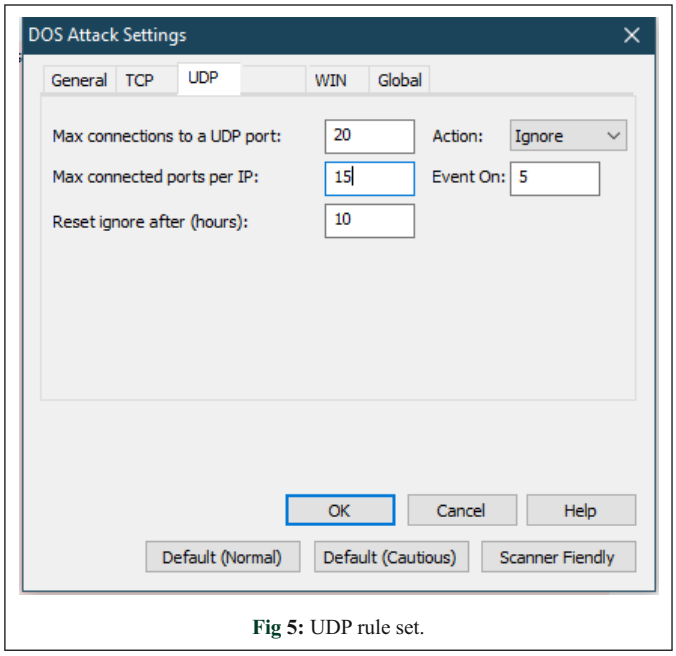

Fig 5: UDP rule set.

Algorithm 2 Algorithm for DMZ network use for external

Input : If external user request
Output : Access specific server
System Initialization;
Receive data packet from external user ;
If DMZrules and Clienrequest=5=True
then
Set GotDMZserver
While Request receive do
Take packet in a certain range;
Create array for input data set;
For Rangeeach do
Sort the data in ascending order;
While Accesstoserver do;
Cheek Firewall rule if match give
Permission to access external;
End
Send Packet toDMZ server;
End
End
End
Discards Request
End

V. DISCUSSION:

A. Signaficance and application:

For our study and work on this paper mitigate DDoS attack because of the day by day thousand and million and million Traffic generates each of a single minute if in this process run on continue it happened to our security loss. Now we perform daily work based on the Internet, without the internet we cannot move on.so we have to secure our data security as well as our system. This work can help to solve the regarding problem and secure our data. This application based on mitigates DDoS attack and work significantly if all layer works together.

Nowadays, IoT devices can increase so our system became vulnerable we must protect the malicious traffic as well as a hacker.so we looking forward to trying how our system security in this application can able to solve some relevant problems to the basis of the current problem.

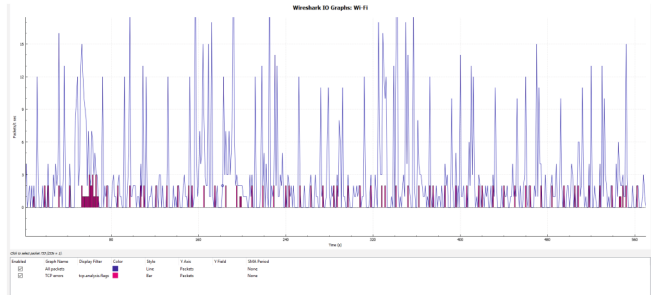

Fig 6: Without rule traffic flow.

Fig 7: With rule traffic flow.

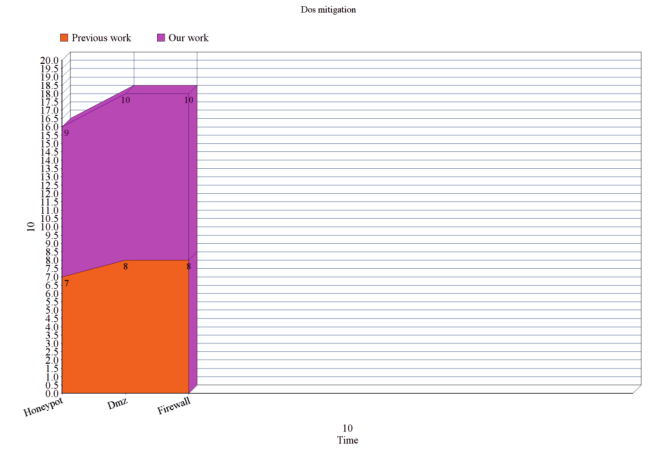

Fig 8: Comparison between previous work.

Table 1: Simulation results.

Number of (Req :)	TCP ports	UDP ports	Without proposed	Proposed system	Efficiency rate
10	7	3	10	5	95%
50	35	15	50	45	92%
60	45	15	60	55	91%
85	55	30	80	40	88%
100	90	10	100	20	87%

B. Scope and limitation:

We focused on mitigating DDoS attack we create an application and create a layer for this purpose it works well if manage all layers work together otherwise it not work efficiently it works well on the small network not large areas of the network like government.

C. Future work:

Looking forward to making an application and system to doing work well for large areas of network and reduce layer. Because if we extend layer cost will be increasing so we can create a minimum layer and work well.

VI. CONCLUSION:

Well, recapitulate that, Day by day increasing IoT devices as well generate large scale traffic every moment.so we need to concern firstly our data security as well system.so on this situation, in this paper, we work on basically mitigating DDoS attacks using rule-based applications. At first, we detect malicious traffic and block it if the IP did not include in our system database. And we create another system for the external user that is DMZ areas. Here also we set some rule and authentication system if an external user entering our system it can be verified to system rule after that enter to the system. Overall our application can able to gradually work well if all layered work together and correctly manage rule then it works well.

REFERENCES:

I. E. Hodo et al., "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System," pp. 4–9, 2020.

II. G. S. Matharu, "The Internet of Things : Challenges & Security Issues," pp. 54–59, 2014.

III. B. P. Rimal, E. Choi, and I. Lumb, "Chapter 2 A Taxonomy , Survey , and Issues of Cloud Computing Ecosystems," pp. 21–46, 2010, doi: 10.1007/978-1-84996-241-4.

IV. D. J. Nallathambi, "Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks," pp. 8–11, 2017.

V. S. M. Khattab, C. Sangpachatanaruk, D. Moss, and M. Taieb, "Roaming Honeypots for Mitigating Service-level Denial-of-Service Attacks ," 2004.

VI. V. V Das, "Honeypot Scheme for Distributed Denial-of-Service Attack," doi: 10.1109/ICACC.2009.146.

VII. L. M. Vaquero, L. Rodero-merino, J. Caceres, and M. Lindner, "A Break in the Clouds : Towards a Cloud Definition," vol. 39, no. 1, pp. 50–55, 2009.

VIII. A. Behl, "Emerging Security Challenges in Cloud Computing An insight to Cloud security challenges and their mitigation," pp. 217–222, 2011.

IX. K. Shridhar and N. Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot," vol. 3, no. 11, pp. 2378–2383, 2014.

X. N. Weiler, "Honeypots for Distributed Denial of Service Attacks," 2002.

XI. H. A. Deshpande, "HoneyMesh : Preventing Distributed Denial of Service Attacks using Virtualized Honeypots," vol. 4, no. 08, pp. 263–267, 2015.