JURNAL EMACS
[Engineering, MAthematics and Computer Science] Vol.2 No.3 September 2020: 123-127 e-ISSN: 2686-2573

Security Testing Using Intrusion Detection System in Cloud Computing

Augustin Anggeliung[1], Arief Dwi Rachmadian[2], Vincent[3]

[1,2,3] Computer Science Department, School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480
augustin.anggeliung@binus.ac.id;
arief.rachmadian@binus.ac.id;
vincent028@binus.ac.id

Abstract – *The development of technology is very fast, one of them is cloud computing. Cloud computing has been used from various circles and began to be developed. There are various problems that arise in cloud computing, such as problems from data, whether the data will be safe. To ensure that the data is safe, several methods or tools can be used. In this scientific work we use the Intrusion Detection System as an aid tool needed to access the network, including whether packages can protect data in cloud computing. Although the intrusion detection system there are still some shortcomings such as only being able to read some data and the performance will decrease the data very much. To overcome this it is necessary to use several additional tools such as the Intrusion Prevention System which is a refinement of the Intrusion Detection System and using the AES algorithm.*

Keywords: *Cloud Computing; Cyber Security; Intrusion Detection System.*

I. INTRODUCTION

Cloud computing has been circulating widely among the public be it developers, employees, students and others that can happen because of the rapid growth of technology. Cloud computing began to be developed in the field of augmented reality, web-based email systems (eg Yahoo, Google Mail, etc.), online networking sites (eg Facebook, Twitter, LinkedIn, etc.), computing offers a variety of conveniences, for example in the business sector who want to offset the lower operating costs when using cloud computing. Cloud computing not only offers lower costs but also offers practicality in its use so that you as a user can use it anytime and anywhere while connected to the internet this happens because the data is centralized on one system

Cloud computing has several security issues that are often discussed by various groups (Ali, Khan, & Vasilakos, 2015). These security issues include vulnerability to intrusion, loss of data, data retrieved without permission that has the account and privacy of users. Violations from year to year continues to increase, this happens because hackers continue to look for a mistake from the cloud computing architecture.

According to the cyberthreat.id site, a lot of data was leaked because hackers who wanted to take advantage of data recorded

In 2019 Capital One experienced a big data leak after former Amazon web service employees gained access to 140 thousand Social Security numbers, 1 million Social Insurance numbers, and 89 thousand bank account numbers by using a web application firewall that is not configured (Rahman, 2019).

Table 1. Cloud Computing Service

No	Service Model	Describe	Provider
1.	SaaS (Software as a Service)	A service that provides software	Google Apps, IBM, Microsoft 365,
2.	PaaS (Platform as a Service)	A service in the form of a platform that users can use to create applications	Amazon Web Service, Google Apps,
3.	IaaS (Infrastructure as a Service)	A service that offers a physical box server and virtual computer	VMware, CSC, Bluelock

Users of cloud computing may still be unsure because their data will not be safe from data privacy issues unknown to the user, whether the data will be sold or used

as needed will require users. Therefore this privacy issue must have a system design standard that can maintain the security of their data (geeksforgeeks.org)

To help secure data from hacking we use the intrusion detection system as a network monitoring tool. Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and warning issues when the activity is found. This application is able to detect a malicious attempt or a dangerous activity or policy violation. The results will be collected centrally which will later be reported to the administrator (geeksforgeeks.org, n.d.).

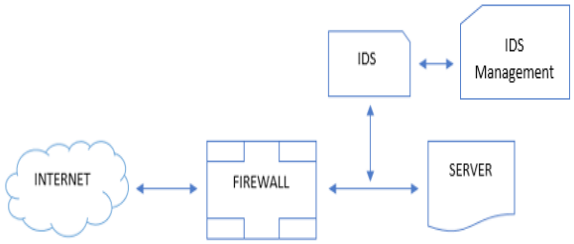

Figure 1 Intrusion Detection System

Intrusion Detection System (IDS) classification is divided into several types, namely Network Intrusion Detection System (NIDS), Host Intrusion Detection System (HIDS), Protocol Based Intrusion (geeksforgeeks.org, n.d.). NIDS (Network-based Intrusion Detection System) is a hardware tool that includes network detection capabilities. Usually it will consist of hardware sensors located at various points along the network. its job is to monitor and analyze traffic across subnet networks, where this NIDS will capture all traffic such as sniffers. To collect all traffic on a network, the implementation can use network beats or mirror ports, where the point is to send a copy of all traffic on the network to IDS. HIDS (Host-based Intrusion Detection System) is the activity of individual network hosts that will be monitored and carried out attacks or intrusion attempts. HIDS are often placed on critical servers on the network, such as those approved by firewalls, web servers, or servers connected to the Internet

Many scientific experts have researched about cloud computing, starting from what is cloud computing, how it is implemented, and others (Wang, 2016). There is a

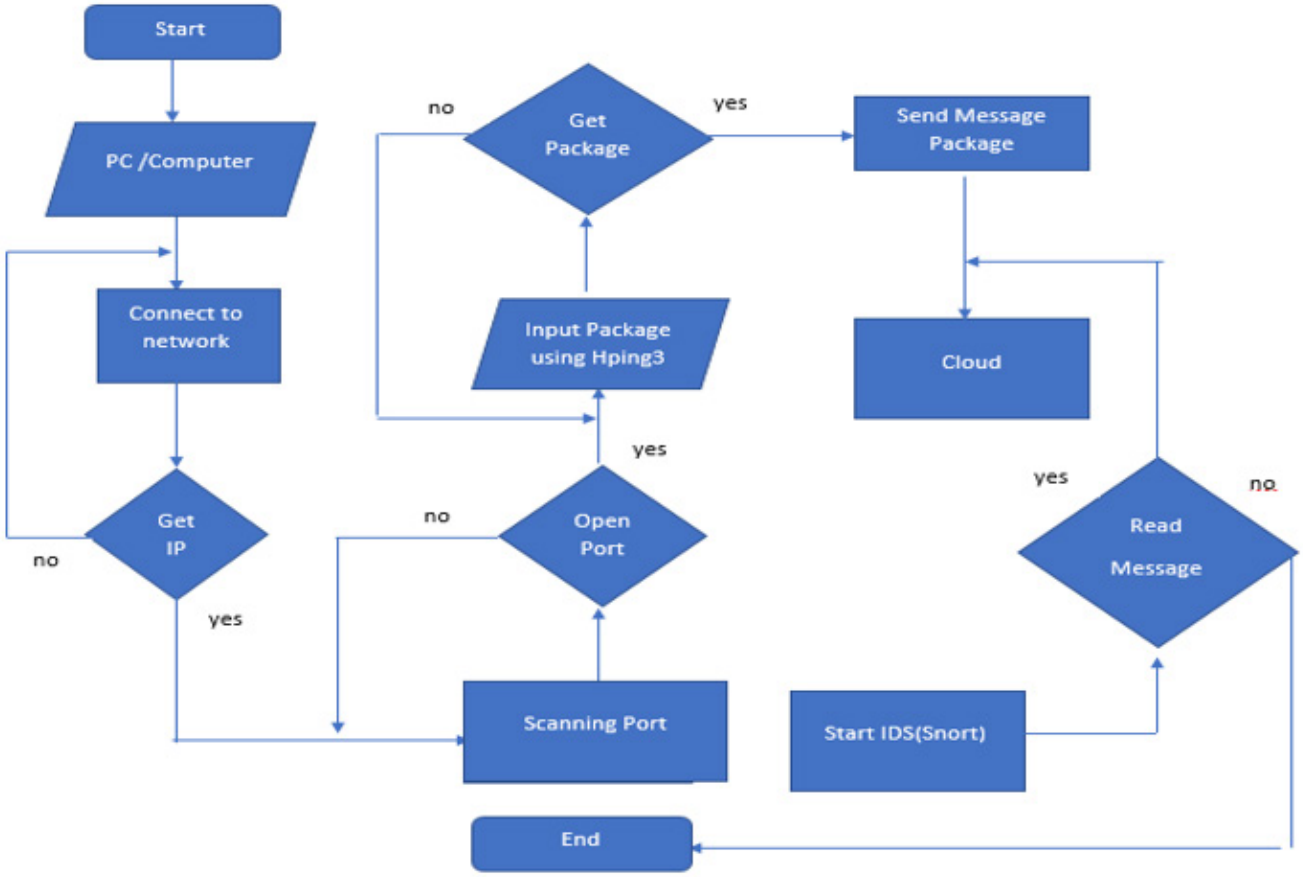

Figure 2 Flowchart how to Intrusion Detetection System work

problem that says that cloud computing is very vulnerable to attacks or hacking by irresponsible people who endanger users and providers of cloud computing services (Baykara & Das, 2018) (Ventkatesh, 2018).and cloud computing can run on mobile platforms (Babu & Kumar, 2018).

After users are worried about the security of their data stored in cloud computing, data security for users is very important especially from the privacy of the data itself because users do not know for sure whether the data will be safe, despite prior agreements regarding privacy. that data. For this reason, cloud computing service providers must maintain the privacy of users (Tchifilionova)

We agree with the use of many methods used to maintain data security and privacy in cloud computing. There are several methods that can be used such as the most popular security techniques including SSL Encryption (Secure Socket Layer), Intrusion Detection

System (IDS), Multi Tenancy Based Access Control (Jakimoski, 2016). Development can be done in many ways one of which can use an experimental testbed, It was compiled by the HP CS 250-HC Virtual Store Blade server, with 4 blades and a malicious Code that we injected into the virtual machine service (Amato, Moscato, Moscato, & Colace, 2017).

We try to use the Intrusion Detection System (IDS) to monitor networks connected to cloud computing. The goal is to find out whether there is something in the network that can endanger data contained in cloud computing.

In IDS there are still several different features ranging from frameworks such as Snort, IDS-AM-Clust, etc. In cloud computing it is necessary to provide an IDS architecture that can be developed which can later be used in cloud computing (Khan & Al-Yasir, 2016). In testing we used Ddos as an attack unit which would later be read by IDS using a Virtual Machine (Khan & Al-Yasir, 2016)

Some of the ways that this is done based on attacks known honeypot has great potential for technological advances, especially in security which can later make cloud computing more secure than hackers and this honeypot method was created by a security community (Saadi & Chaoui, 2016).

Some datasets such as DARPA98, KDD99, ISC2012, and ADFA13 are often used by scientists to evaluate the performance of IDS

which results cannot read all types of attacks (Sharafaldin, Lashkari, & Ghorbani, 2018). For this reason, we use several data sets that allow us to read the general types of attacks.

One of the enhancement applications of IDS is the Intrusion Prevention System (IPS), IPS can be implemented anywhere such as a web server, the purpose of which is to read attacks

that will feed the web (Farhaoui, 2016). only and are in the same lane with a firewall.

We also suggest that developers can use multiple authentication and implement the AES algorithm that can be implemented on heroku as a cloud that was built using PHP applications. In heroku, there are 2 Encrypt & Decrypt Files and Encrypt & Decrypt Text menus. The data can be in the form of files such as .jpeg, .doc, .txt, the results of the file will be encrypted (Lee, Dewi, & Wajdi, 2018).

In the future the development of blockchain-based cloud computing will probably become a reality because many scientists have begun to use blockchain to become a security in cloud computing. There are challenges and obstacles that await in developing blockchain (Park & Park, 2017).

II. METHOD

2.1. Using Intrusion Detection System (IDS)

Using IDS as a monitoring tool is the right choice because it has several capabilities that can be used when implemented in cloud computing, in this paper we will explain the steps to use from IDS and give a little picture of the results that have been tested

In Figure 2 shows a flowchart of what will be done in this attack and how to implement an IDS in reading the attack using the DDos attack type to flood the network with fake requests.

The tools needed to implement attacks use ddos and IDS as a reader for this type of attack, although what is needed is a virtual machine, PCBSD, Nmap, hping3, Snort. The first step to do is connect your computer to 3 NICs. NIC1 to connect to the internet, NIC2 to connect to clients, and NIC3 to connect to IDS. You can see this by entering the terminal then typing ipconfig to show what is 3nic that you connect.

The IP Address used in this example is 192.168.2.2 This depends on your computer being connected to the network. The purpose of this ip is to carry out attacks that will be read by IDS. For IDS itself, we use PCBSD as a platform to run it.

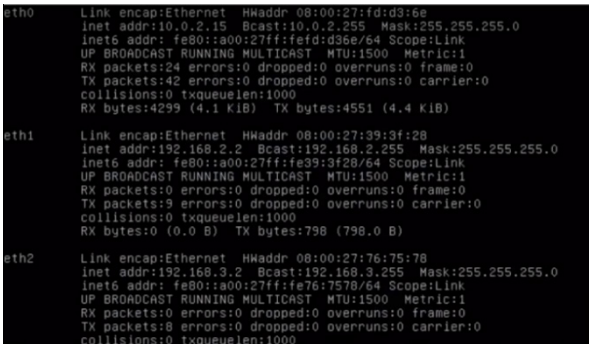

Figure 3 Check 3NIC

Next look for open ports on the server that will be used as the entrance to the network that we will test. to get open ports on the server, we can use the Nmap tool. Nmap is a tool for scanning ports on open servers. the way to type the “Nmap (Ip Address)” command line in this example

is Nmap 192.168.2.2. When scanning a port takes a long time, be patient. When finished, which port will open, the example on this computer will be 111.

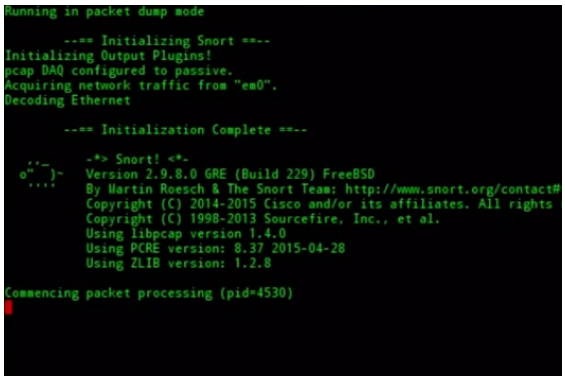

Figure 4 Start Intrusion Detection System

What we need is an open IP address and port, the next step is to make sure that the IDS is active. For IDS we use a kind of framework that facilitates IDS implementation called Snort. to activate the snort the easy way just type the snort then the snort will be activated.

The next step is to test whether the snort is working, we use the ddos method to do the testing with the hping3 tool that is already installed on the PCBSD. How it works from ddos by flooding the network using packets so that the performance of this network can interfere and can reduce performance.

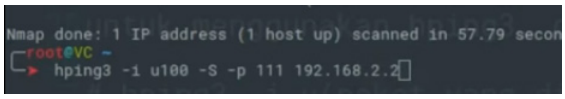

Figure 5 Syntax Hping3 to attack the cloud

To do the hping3 technique as shown in figure 5 we have to type the command in the terminal which contains the command "hping3 -iu (the package is done -S -p [open port] [ip viktim]", then on our computer just try it like this "hping3 - i u100 -Sp 111 192.168.2.2 ". What is meant by u100 is the number of packets that will be loaded into the network to be sent to snort.

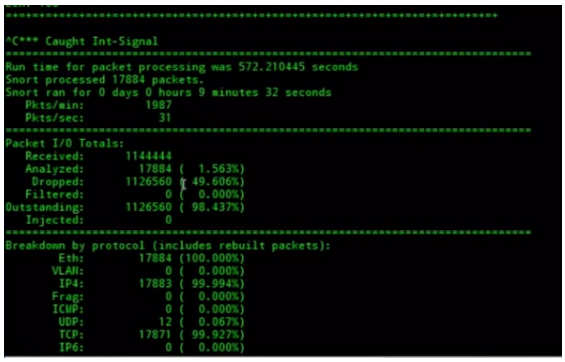

Figure 6 Result From Intrusion Detection System

The results obtained when sending a package to IDS. The time needed to run it all around 572 seconds was quite slow and IDS received data of 1144444 while only 17884 were successfully analyzed. This happened because IDS was unable to provide action but only gave alerts to users. Therefore, we need to install another application that has been developed, namely IPS, it works almost the same as IDS, the only difference lies in the ability of IPS to be able to block a packet if the package is suspicious or has the potential to endanger the user or the data itself.

III. RESULTS AND DISCUSSION

The results of the picture show a large enough number in which the package received into hundreds of thousands, but it is unfortunate to be analyzed using IDS only about a dozen tens. This can happen because the IDS snorts system that cannot control or block suspicious packages as a result, it is just like a CCTV camera that only monitors if there are suspicious people who are only able to give a warning.

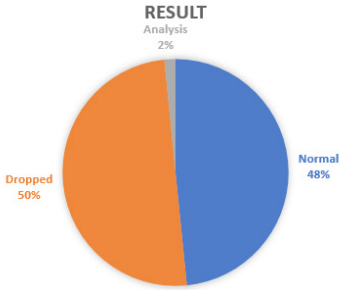

Figure 7 Percentage Intrusion Detection System

The figure 7 shows that 50% of packages sent to cloud computing have been successfully dropped by IDS Snort. This is done because the suspicious IDS snort or the packet can harm the network or can cause a decrease in the performance of the cloud therefore the IDS dropped the suspicious packet. As for the data that was successfully analyzed by IDS snort, only 2% of this happened because the data entered was too much. The amount of data entered and monitored by IDS is only 17884 out of the total data of almost 1.1 million data entering the cloud. The capacity of IDS when more data comes in, the performance to analyze data will decrease, this is a drawback of IDS, each incoming data is large, then IDS will not be able to analyze the data. Data entering the cloud is 48% which is normal data detected by IDS.

Table 2 Comparison attack type

No	Attack type	Normal	Ddos
1.	Hping3	48%	50%
2.	Honeywall+ honeyd+ID-SAM-Clust	31%	33%

In the table 2 shows the results of other work experiments carried out with different techniques but using the same type of attack that is DDOS which supports to flood the network so that it cannot be used properly. Looking for the hping3 technique with Honeywall + honeyd + IDSAM-Clust, hping3 can produce attacks that are readable by IDS is 50% while other techniques produce 33%. Actually the results obtained are average when viewed from the amount of data that comes in and data that comes out, at hping 3 the

normal data is 48% and the abnormal data is 50% while in other techniques the normal data is 31% and the abnormal is equal to 33% if we compare the data that comes in and the data that comes out is always bigger the data that comes out. This happens depending on the amount of data that is entered and read by the IDS.

Because IDS has a problem if the data is too large, you can add additional tools like IPS. The fundamental difference is that IPS can receive and analyze data larger than IDS.

IV. CONCLUSION

The conclusion of this scientific work is that with the increasing use of cloud computing, there must be technology that is able to overcome the problem of cloud computing security, because it would be very dangerous if the service provider paid less attention to it. The use of IDS can be very helpful in combating thieves who want to retrieve data from cloud computing, although there are still deficiencies such as IDS that is only able to detect intruders but cannot provide action, but no need to worry because there is an IPS that can detect and block suspicious activity. What we have done is only limited to basic level testing or implementation of a dos-based assault model and uses IDs as network traffic monitors. because there are still deficiencies that exist it would be better if cloud computing developers can use additional security such as dual authentication, applying the AES algorithm and in the future can use blockchain as a security tool in cloud computing, and more security systems are used in cloud computing then the results will be better

REFERENCES

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Elsevier*, 357-383.

Amato, F., Moscato, F., Moscato, V., & Colace, F. (2017). Improving Security in Cloud by Formal Modeling of IaaS Resource. *Elsevier*, 754-764.

Babu, V. S., & Kumar, M. M. (2018). An Efficient and Secure Data Storage Operations in Mobile Cloud Computing . *IJSRSET*.

Baykara, M., & Das, R. (2018). A novel honeypot based security approach for real-time intrusion detection and prevention system. *ELSEVIER*, 103-116.

Farhaoui, Y. (2016). How to secure web servers by the intrusion prevention system (IPS). *International Journal of Advanced Computer Research*, 2277-7970.

geeksforgeeks.org. (t.thn.). *Intrusion Detection System*. Diambil kembali dari geeksforgeeks: https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing. *International Journal of Grid and Distributed Computing*, 49-56.

Khan, N., & Al-Yasir, A. (2016). Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. *ELSEVIER*, 485-490.

Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018). Data Security in Cloud Computing Using AES Under HEROKU Cloud. *IEEE*.

Park, J. H., & Park, J. H. (2017). Blockchain Security in Cloud Computing: Use Cases,Challenges,and Solutions. *Symmetry*, 9.

Rahman, A. (2019, Desember 13). *2019 Data Violations Caused by Internal Persons*. Diambil kembali dari Cyberthreat: https://cyberthreat.id/read/4221/Pelanggaran-Data-Tahun-2019-yang-Diakibatkan-Orang-Internal.

Saadi, C., & Chaoui, H. (2016). Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. *ELSEVIER*, 433-442.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *SCITEPRESS*, 108-116.

Subhashini, D. P. (2018). A Study on Cloud Computing Securities and Algorithms. *International Journal of Scientific Research in Compter Science, Engineering and Information Technology*, 2456-3307.

Tchifilionova, V. (t.thn.). Security and Privacy Implications of Cloud Computing – Lost in the Cloud. *National Laboratory of Computer Virology, Bulgarian Academy of Sciences 1113 Sofia*.

Ventkatesh, M. S. (2018). A Study of Data Storage Security Issues in Cloud Computing. *Vosal*.

Wang, R. (2016). Research on data security technology based on cloud storage. *13th Global Congress on Manufacturing and Management*.