Enhancing Secure Cloud Computing Environment by Detecting DDoS Attack Using Fuzzy Logic

Himadri Shekhar Mondal*, Md. Tariq Hasan, Md. Bellal Hossain, Md. Ekhlasur Rahaman and Rabita Hasan
Electronics and Communication Engineering Discipline, Khulna University, Khulna, Bangladesh.
*bdhimadri@gmail.com

***Abstract*—Cloud computing has become a part and parcel of our daily life. It just made our life easier with its amazing features. To support increasing number of users as well as smart devices, it is needed to keep the cloud environment more and more secure and reliable. Cloud computing security has become a major challenging field now a days. In this paper we presented a Fuzzy based mechanism, which may be helpful for the detection of Distributed Denial of Service (DDoS) attack in cloud computing environment. As DDoS attack becomes powerful with the passing of time, if it is detected at first, then the attack may be minimized. So we focused on attack detection mechanism to secure the cloud environment using Fuzzy logic.**

***Index Terms*—Cloud computing environment, Fuzzy logic, DDoS attack.**

I. Introduction

Present world is blessed with computing technology. Cloud computing technology has added a new dimension in the internet based system with its adaptive and reliable features. Without the rise of cloud computing, it may not possible to enjoy high speed internet for the increasing number of users. Now a days increasing security has become a major challenging factor for service providers. The anomalous attack is going on which damages both the money and valuable time. If it is possible to mitigate the attacks in the cloud system, then, the end users will enjoy the beauty of secure cloud environment more perfectly.

There are many types of attack, which may destroy the cloud environment within a second if there is no preventing mechanism. The most common attack in cloud environment is Distributed Denial of Service (DDoS) attack. This attack targets the machine running in a networking system and generates large number of traffics. These traffics attacks the server system in the cloud environment. The cloud servers suddenly get pressurized as it has to process huge number of traffic. If there is no prevention mechanism in the cloud system, then, the packet arrival rate becomes high with the increasing of time. As a result, at one stage, the cloud system fails to serve its users.

We proposed a Fuzzy based mechanism to detect the attack in the cloud system. We know Fuzzy system is used to reduce the human brain pressure, as it can perform logical operation like human brain can do. So it is possible to detect the anomalous behavior of packets if we implement the Fuzzy logic in the cloud system. All the incoming data will be filtered through the Fuzzy system before arriving in the cloud environment. A Fuzzy logic based IF-THEN rule is implemented in the Fuzzy inference engine system which will analyze the incoming data packet behavior and send the report to the cloud system. If there is huge number of data, which load seems to heavy for the cloud environment, the defense mechanism may active or the data may be discarded by the cloud system automatically. Thus, the cloud system can provides secure, friendly and reliable service to its users.

In this paper we mainly focused on DDoS attack detection mechanism using Fuzzy logic. The outline is designed as, related works are discussed in section II, the methodology of the proposed system is presented in section III. The results are discussed in section IV, where we have presented results by changing the parameters. Section V is based on conclusion and future works.

II. Related works

Plenty of research works are going on to ensure the secure cloud environment. The history of developing this attack mechanism was observed on 1980s, a network research group discovered that internet control message protocol (ICMP) packets making the network complex for the users, which is marked as the concept of DDoS attack. The DDoS attack first traced in June, 1998 by a group of network researchers [1]. Lo *et al* [2] presented a method which is based on Intrusion Detection System framework. Bakshi *et al* [3] presented a secure cloud computing model which can prevent the DDoS attack. N. Jeyanthi [4] proposed a model using Packet Resonance Strategy (PRS) which can be helpful for preventing the DDoS from spoofed address. Chen *et al* [5] proposed a filtering technique to prevent the DDoS attack. S. Chavan [6] presented a Intrusion Detection System (IDS) which is based on neuro-fuzzy system.

The Fuzzy system was first invented by L.A. Zadeh [7] at 1965. The proposed system was not good enough then and didn't gain much popularity. He then started research again to improve the system. As a result his landmark paper [8] was published on 1973. The reason of popularity was much more effective when Mamdani [9] applied his inference engine rule on the Fuzzy system.

Lee *et al* [10] presented the security techniques in cloud system. Zhu *et al* [11] presented a Fuzzy based authorization system in cloud computing architecture. A. Visconti *et al* [12] presented a Fuzzy based algorithm, which collects data from various networking elements and detects the misbehaving nodes by comparing the collected data. Watkins et al [13]

978-1-5386-2307-7/17/$31.00 ©2017 IEEE

also presented a comparison based attack techniques in cloud computing environment using Fuzzy system. Lou *et al* [14] discussed the piracy prevention techniques in Content Delivery network. Research challenges in cloud system were presented by Boutaba *et al* [15].

III. Methodology

In this section we've discussed our proposed methodology for detection of DDoS attack in cloud environment.We've mainly proposed a system which needs to implement in the cloud environment for a quick detection of attacks and ensure the safe working environment. In the system we've taken three inputs and calculated one output. In the input section, entropy of source IP, port address and packet arrival rate are considered. Using these parameters we have shown attack status based on Fuzzy IF-THEN rules. The entropy is calculated mainly based on Shannon's theorem [16], which indicates that, If a source is independent and the source carries *n* variables having the probability of P_i, then the entropy *E* will be calculated through this equation,

$$E = -\sum_{i=1}^{n} P_i log_2 P_i \tag{1}$$

DDoS attack targets the remote servers and attacks the machines with a huge number of packets. If the attack can gain the access of central server by bypassing the vulnerable security system, then it creates a huge number of fake traffic which is impossible to handle for the central server system of cloud. As a result, new arrival packets can't be processed by the machine and have to face the anomalous environment for the user. With the passing of time the attack becomes higher, so it is possible to minimize the attack if it is identified at the beginning. If we use Fuzzy system in the cloud environment then it can detect the anomalous behavior of the incoming packets. As we know, Fuzzy system is helpful for decision making criteria, it can help to reduce the human thinking, we can easily implement it. We considered the different protocols [17] like Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP) User Datagram Protocol (UDP) etc.

The Fuzzy system has three stages in its working principle. They are,

1) Fuzzification
2) Inference mechanism
3) Defuzzification

In the Fuzzy system the crisp values are needed to be converted for the calculation, and this work is done by the fuzzification steps. The fuzzified values are then used by inference engine, which actually maps the data systems using the logistic operations. Finally the defuzzification system converts the fuzzified values to the crisp values. For our better realization, consider a Fuzzy set F which has Z elements, these values are mapped pair domains and remains between the value of 0 and 1. Mathematically we can written as,

$$F = \{(z_1, 0.6), (z_2, 0.4), (z_3, 0.2), (z_4, 1)\} \tag{2}$$

Using Zadeh's [8] notation we can write this equation as,

$$F = \{\frac{0.6}{z_1} + \frac{0.4}{z_2} + \frac{0.2}{z_3} + \frac{1}{z_4}\} \tag{3}$$

The membership function is used to mapped the data according to their values in the rule base inference engine. Let us consider a membership function μ_F , which will map the elements of Z in between 0 and 1. Mathematically this can be written as,

$$F = \{(z, \mu_F(z)) \,|\, z \,\epsilon\, Z\} \tag{4}$$

The basic block diagram of Fuzzy system in presented in Fig. 1.

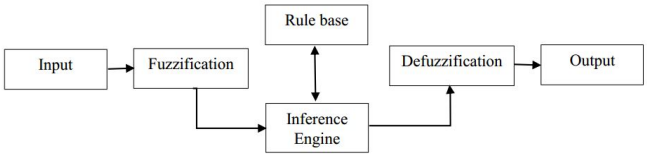

Fig. 1. Fuzzy basic block diagram

1. Fuzzification

The fuzzification is the first step in the fuzzy system in which the inputted values are converted to the fuzzified values. This system may work in the two ways.

Let consider F_{ui} is the Fuzzy singleton, so we can express it as,

$$F_{ui}(u) = \begin{cases} 1 & if\ u = u_i \\ 0 & otherwise \end{cases} \tag{5}$$

Also, if F_{ui} is Fuzzy set, then,

$$\mu_{F_{ui}} = \begin{cases} 1 & if\ u = u_i \\ decrease\ from\ 1 & when\ moving\ from\ u_i \end{cases} \tag{6}$$

2. Inference Engine

Fuzzy inference engine is the heart of the Fuzzy system as the logic based operation is performed here. We choose Mamdani [9] type inference which is a popular and widely used inference engine. The basic rule for inference engine is,

IF x is A and y is B THEN z is C

Here we have more than two input. In this type of case, the output will be the minimum membership degree of the input parameters. We have implemented Fuzzy based IF-THEN rule in the inference system which can be presented as,

IF *Entropy of Source IP is* {*Low, Medium, High*} ***AND*** *Port Address is* {*Low, Medium, High*} ***AND*** *Packet Arrival Rate is* {*Low, Medium, High*} ***THEN*** *the attack type is* {*Low, Medium, High*}

According to IF-THEN rule we designed a rule based lock which is presented in the table 1.

Table 1: Fuzzy based implemented IF-THEN rule

EoSIP (i)	PA (i)	PAR (i)	AS (o)
Low	Low	High (ICMP)	High
Low	(none)	High	High
High	High	Low	Medium
Low	Low	High (UDP)	High
Low	High	High	High
Medium	Medium	High	High
High	High	High	High
Low	Medium	Low	Low
Low	High	Medium	Medium
High	Medium	Medium	Low
High	Medium	High	Medium
Low	Medium	High	High
High	Low	Medium	Low
Low	Low	Medium	Medium
Medium	Low	Low	Low
Medium	Low	High	High
Medium	Medium	Low	Low
High	Medium	Low	Low

Here in this Table 1, EoSIP refers to Entropy of Source IP, PA indicates Port Address, PAR refers to Packet Arrival Rate, AS indicates Attack Status, i indicates the inputs and o indicates the output.

3. Defuzzification

The defuzzification is needed for converting the fuzzified rule based values to the crisp values. This reverse process of fuzzification system helps to determine the values to the readable values for the calculation.

The Fuzzy system described here is used to determine the attack status in the cloud environment. As heavy packets generates by the DDoS attacker, the main target is to detect the attack at its earlier stage. If earlier detection is possible then it is possible to mitigate the attack for ensuring secure cloud environment. The Fuzzy system including cloud environment is presented in the Fig. 2.

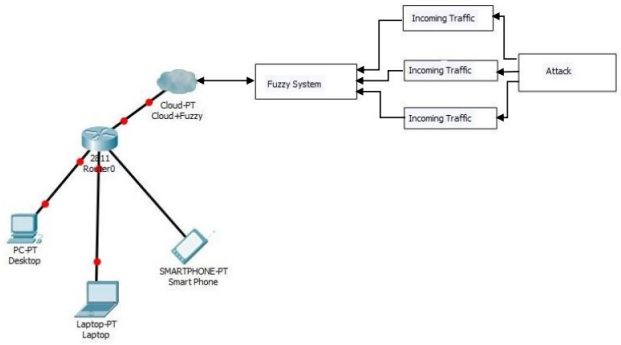

Fig. 2. Implemetation of attack detection model

.

IV. Result

The Fuzzy IF-THEN rule is implemented using Matlab software and the result is shown here. The figure 3 is based on normal value which shows the surface base view.

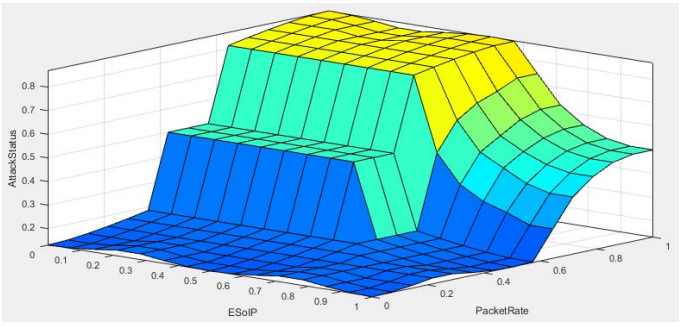

Fig. 3. Attack status at normal stage

Figure 4 is just the representation of figure 3 as rule base view,

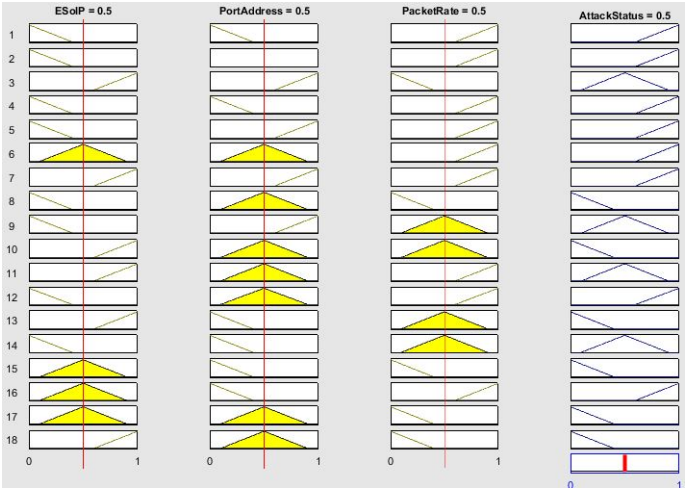

Fig. 4. Rule base relationship status

Here all the value remains between 0 and 1, we considered 0 as the minimum value and 1 as the maximum value also, 0.5 is considered as the normal value. Now let increase the packet arrival rate, the result is shown in figure 5.

From the figure 5, we can see that, due to increase of the packet arrival rate, the attack status becomes high. Now lets increase the entropy of source IP. the result is shown in the figure 6.

From the figure 6, we can see as soon as we increase the entropy of source IP, the attack status decrease from its previous increased stage. So we can easily determine the attack status in cloud computing environment by implementing Fuzzy logic.

There are so many DDoS attack detecting mechanisms but, the Fuzzy logic implemented mechanism is cost effective, reliable and easy method for the cloud system. The cloud environment has to deal with a huge number of process for providing better service to its users, so if we implement a heavy method for attack detection, then the user may not get desired service from the cloud. As this Fuzzy logic is easy and

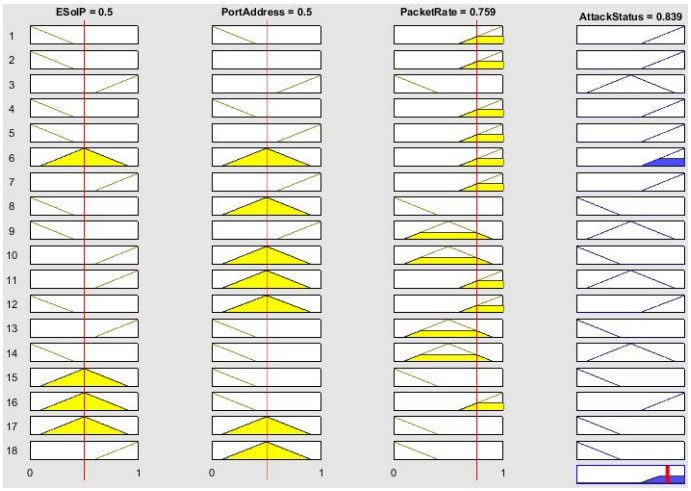

Fig. 5. Packet arrival rate increased

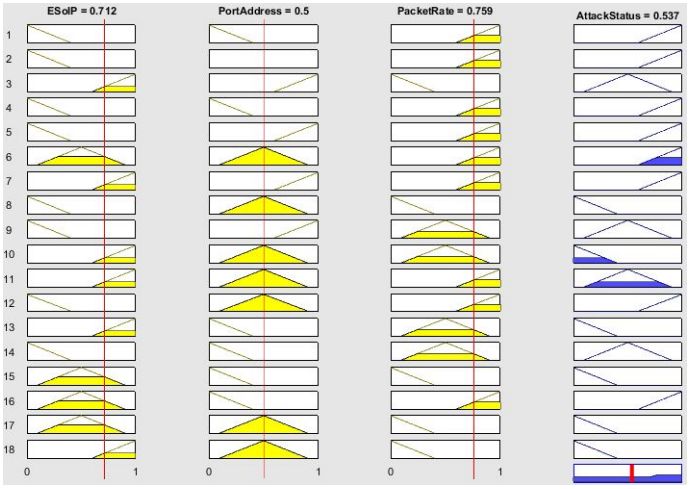

Fig. 6. Attack status due to changing of parameters

reliable, then it can be easily implemented in cloud computing environment to ensure secure cloud environment for its users.

V. Conclusion

Attack in cloud computing may be minimized but early detection is needed, which is presented in this paper. The attackers always try to discover a way to bypass the security system to make the system vulnerable. So the security system may need more research to prevent the new discovered attacks. It is possible to acquire more fruitful result in the future by adding more variable using the Fuzzy system, which will be more reliable, dynamic and provide better secure performance for the users.

References

[1] S.-C. Lin and S.-S. Tseng, "Constructing detection knowledge for ddos intrusion tolerance," *Expert Systems with applications*, vol. 27, no. 3, pp. 379–390, 2004.

[2] C.-C. Lo, C.-C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *Parallel processing workshops (ICPPW), 2010 39th international conference on*, pp. 280–284, IEEE, 2010.

[3] A. Bakshi and Y. B. Dujodwala, "Securing cloud from ddos attacks using intrusion detection system in virtual machine," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, pp. 260–264, IEEE, 2010.

[4] N. Jeyanthi and N. C. S. Iyengar, "Packet resonance strategy: a spoof attack detection and prevention mechanism in cloud computing environment," *International Journal of Communication Networks and Information Security*, vol. 4, no. 3, p. 163, 2012.

[5] Q. Chen, W. Lin, W. Dou, and S. Yu, "Cbf: a packet filtering method for ddos attack defense in cloud environment," in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, pp. 427–434, IEEE, 2011.

[6] S. Chavan, K. Shah, N. Dave, S. Mukherjee, A. Abraham, and S. Sanyal, "Adaptive neuro-fuzzy intrusion detection systems," in *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, vol. 1, pp. 70–74, IEEE, 2004.

[7] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.

[8] L. A. Zadeh, "Outline of a new approach to the analysis of complex systems and decision processes," *IEEE Transactions on systems, Man, and Cybernetics*, no. 1, pp. 28–44, 1973.

[9] E. H. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," *International journal of man-machine studies*, vol. 7, no. 1, pp. 1–13, 1975.

[10] R. K. Ko, M. Kirchberg, and B. S. Lee, "From system-centric to data-centric logging-accountability, trust & security in cloud computing," in *Defense Science Research Conference and Expo (DSR), 2011*, pp. 1–4, IEEE, 2011.

[11] S. Zhu and G. Gong, "Fuzzy authorization for cloud storage," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 422–435, 2014.

[12] A. Visconti and H. Tahayori, "A biologically-inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad-hoc wireless networks," *INTERNATIONAL JOURNAL FOR INFONOMICS*, vol. 3, no. 2, pp. 373–382, 2010.

[13] D. Watkins, "Tactical manet attack detection based on fuzzy sets using agent communication," tech. rep., MORGAN STATE UNIV BALTIMORE MD, 2004.

[14] X. Lou and K. Hwang, "Collusive piracy prevention in p2p content delivery networks," *IEEE Transactions on Computers*, vol. 58, no. 7, pp. 970–983, 2009.

[15] R. Boutaba, L. Cheng, and Q. Zhang, "On cloud computational models and the heterogeneity challenge," *Journal of Internet Services and Applications*, vol. 3, no. 1, pp. 77–86, 2012.

[16] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001.

[17] B. A. Forouzan, *TCP/IP protocol suite*. McGraw-Hill, Inc., 2002.