ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (193-198), Month: January - March 2015, Available at: www.researchpublish.com

To Implement Intrusion Detection System for Cloud Computing Using Genetic Algorithm

[1]Ku. Shraddha D. Patil, [2]Ku. Sunita S. Ganveer, [3]Ku. Prachi S. Badge

Department of Computer Science and Engineering, Dr. Babasaheb Ambedkar College of Engineering and Research, Nagpur -440010

Abstract: **In this paper, we discuss the cloud security issues. Cloud computing is a "network of network" over the internet, therefore, chances of intrusion is more with the erudition of intrusion attack. Cloud system security is one of the most important issues that have attracted a lot of research and development effort in past few years. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machine to deploy further large-scale Distributed Denial-Of–Services (DDOS). An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of computer system. In a cloud system where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud system and use its resource to deploy attacks in more efficient ways. To overcome this problem we are implementing intrusion detection system in which we use genetic algorithm to identify and detect intrusion and also prevent from attack.**

Keywords: **Cloud computing, network security issue, IDS, Malicious behavior, attack, Packets, analysis.**

I. INTRODUCTION

Cloud computing can be defined as internet-based computing where by shared resources. Software and information are provided to computers and other device on demand. Cloud computing has been rapidly developed along with the trend of IT services. A cloud computing service is a new computing paradigm in which people only need to pay for use of services without cost of purchasing. In recent times, information system security has become a growing concern as computer system worldwide become increasingly vulnerable or open to harm due to the rapid increase in connectivity and accessibility, which has indirectly resulted in more frequent intrusions, misuses and attacks. Intrusion detection attempts to detect computer attacks by inspecting data records observed by processes on the same network [1].

Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. cloud computing provides a framework for supporting end users easily attaching powerful services and applications through internet. Denial-of-services (DoS) attack or Distributed Denial-of-Services are major security issues in cloud environment. The best solution to protect the cloud from these attacks is use of IDS [4].

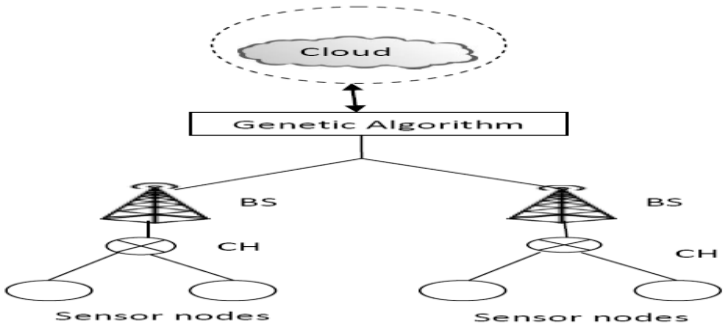

Figure (1): System Architecture

The above figure shows overall concept of project. In which there are multihop network c1, c2, c3 are connected with each other. The data packet transfer from c1 to c2 then c2 to c3 which is called multihop forwarding. Before forwarding data packet of c3 to the cloud network in which genetic algorithm is use. This algorithm check the packet size, multiple request of data packet and number of files. Here packet size is 128KB fixed, only one request of data packet and number of files is also one. If it is match then the data packet will be enter in the cloud network. Otherwise data packet will be blocked by applying genetic algorithm.

II. SECURITY ISSUES IN CLOUD COMPUTING

Security has always been the main issue for IT Executives when it comes to cloud adoption. however, cloud computing is an agglomeration of technologies, operating system, storage, networking, virtualization, each fraught with inherent security issues. for example, browser based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing[2]. Security threats can be categorized as follow:-

1. Cloud data confidentiality issue:

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service provider‟s end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case. Above mentioned cloud security issues are a few and dynamicity of cloud architecture are facing new challenges with rapid implementation of new service paradigm.

2. Cloud security auditing:

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

3. Lack of data interoperability standards:

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user‟s data and application may not be compatible with other vendor‟s data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider [1].

III. LITERATURE REVIEW AND RELATED WORK

Author Parag K. Shelke [1] concludes that providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. Distributed model of cloud makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of service (DDOS) and Cross Site Scripting. To handle large scale network access traffic and administrative control of data and application in cloud, a new multithreaded distributed cloud IDS model has been proposed. Our proposed cloud IDS handles large flow of data packet, analyze them and generate reports efficiently by integrating knowledge and behavior analysis to detect Intrusion.

Mohammad sazzadul hoque, md.abdul mukit [5] describes, nowadays it is very important to maintain a high level security to ensure safe and trusted communication of information between various organizations. But secured data communication over internet and any other network is always under threat of intrusions and misuses. So Intrusion Detection Systems have become a needful component in terms of computer and network security. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely. In this progression, here we present an Intrusion Detection System (IDS), by applying genetic algorithm (GA) to efficiently detect various types of network intrusions. Parameters and evolution processes for GA are discussed in details and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity.

S. N. Pawar [3] Describes the intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks since the increased connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification. Intrusion detection systems are used to detect unauthorized access

to a computer system. A number of soft computing based approaches are being used for detecting network intrusion. This paper presents a survey on intrusion detection techniques that use genetic algorithm approach.

Monjur Ahmed and Mohammad Ashraf Hossain [4] Describe security issues in the cloud computing. Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud architecture. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility, and advantages that cloud computing has to offer will have little credibility. This paper present a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing.

IV. PROPOSED WORK

Generate a multi hop cloud network. First we are going to connect the network. each node is connected the neighboring node and it is independently deployed in network area when a packet is generated by the sender the packet get activated .The authenticated user to allow accessing a cloud space for storing or retrieving a file or any application. Cloud networks which generate security event and alerts and control the cloud networks. After this, browse and select the source files and selected data is converted into fixed size of packet and the packet is send from source to destination. Monitoring and analyzing by genetic Algorithm the event occurring in the network in order to detect abnormal activities through genetic algorithm. The intrusion detection is defined as a mechanism for a packet in network to detect the existence of inappropriate, incorrect, or anomalous moving attackers. If the Genetic Algorithm found an anomalous behavior then the packet will be blocked. After filtering the invalid packets will be block and all the valid Packets will reach to the destination. There are several ways to categorize an IDs depending on the type and location of the cloud networks and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

A. CREATE WIRELESS NETWORK:

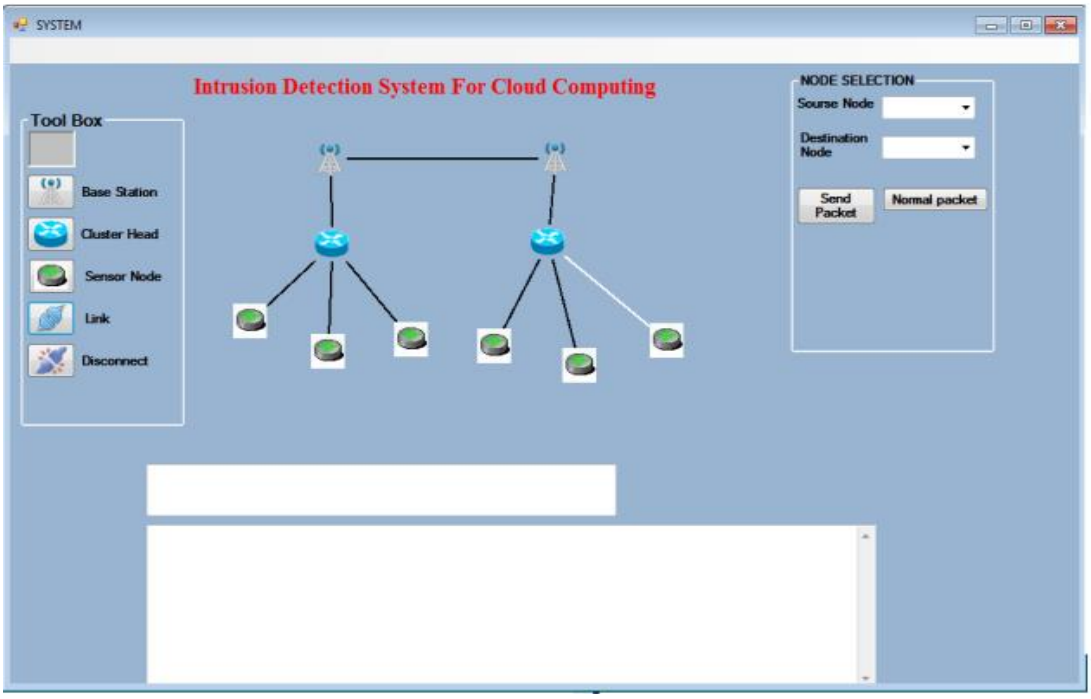

Figure (2)

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (193-198), Month: January - March 2015, Available at: www.researchpublish.com

This is the network scenario of wireless network. Two wireless networks are connected with each other as shown in above figure. There are various tools present to create wireless network. Like base station, cluster head, sensor node, link and disconnect link. Here Node selection is also present for selecting the source node and destination node from node dictionary and show the path for sending packet from source to destination.

B. DATA TRANSMISSION AND RECEPTION IN WIRELESS NETWORK:

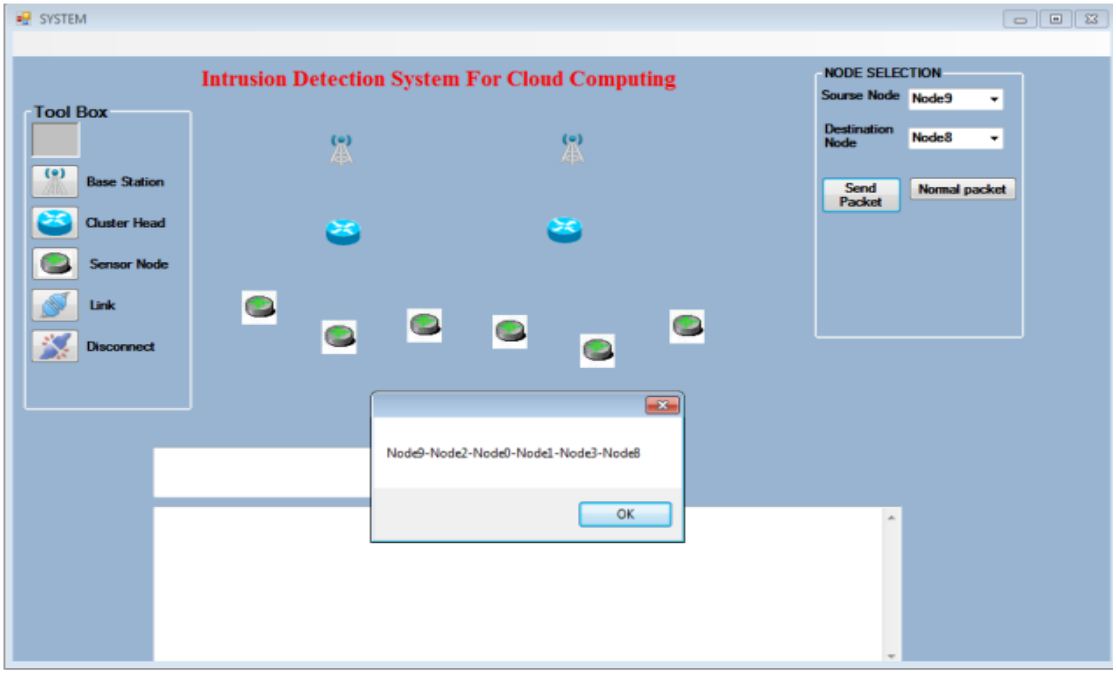

Figure (3)

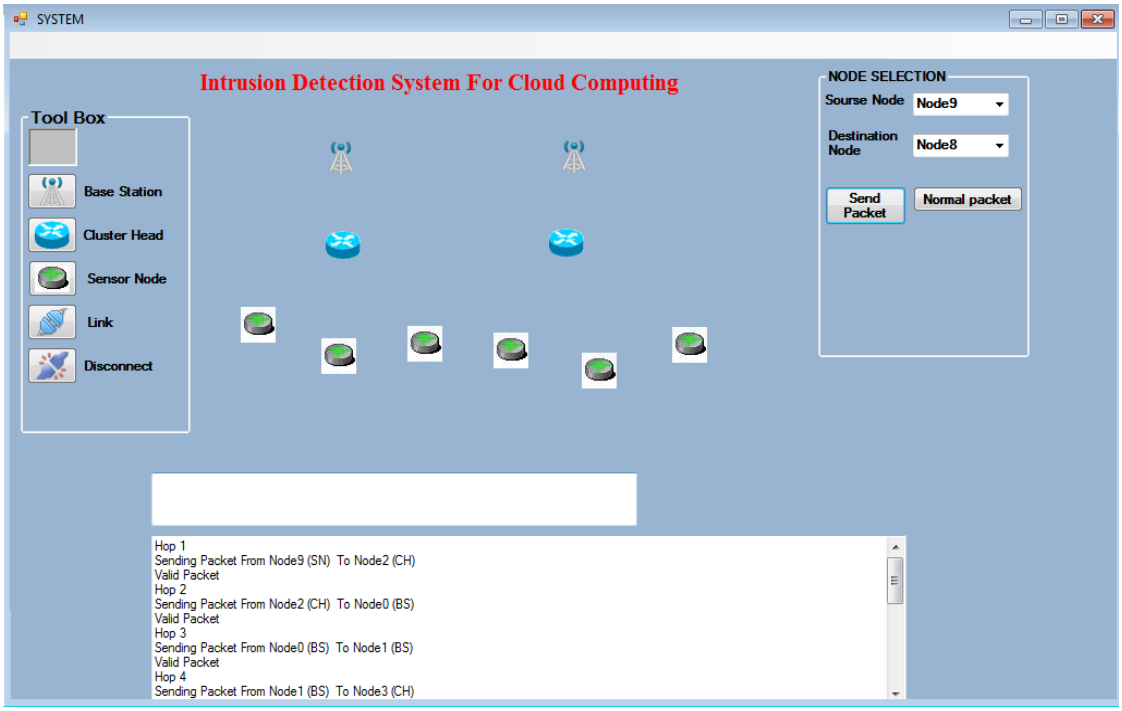

Figure (4)

Figure (b) shows the path on which the packet flowing from source node to destination node. And figure (c) contain the routing table to shows the packet valid or invalid at each hop.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (193-198), Month: January - March 2015, Available at: www.researchpublish.com

C. MONITORING AND ANALYZING THE PACKET:

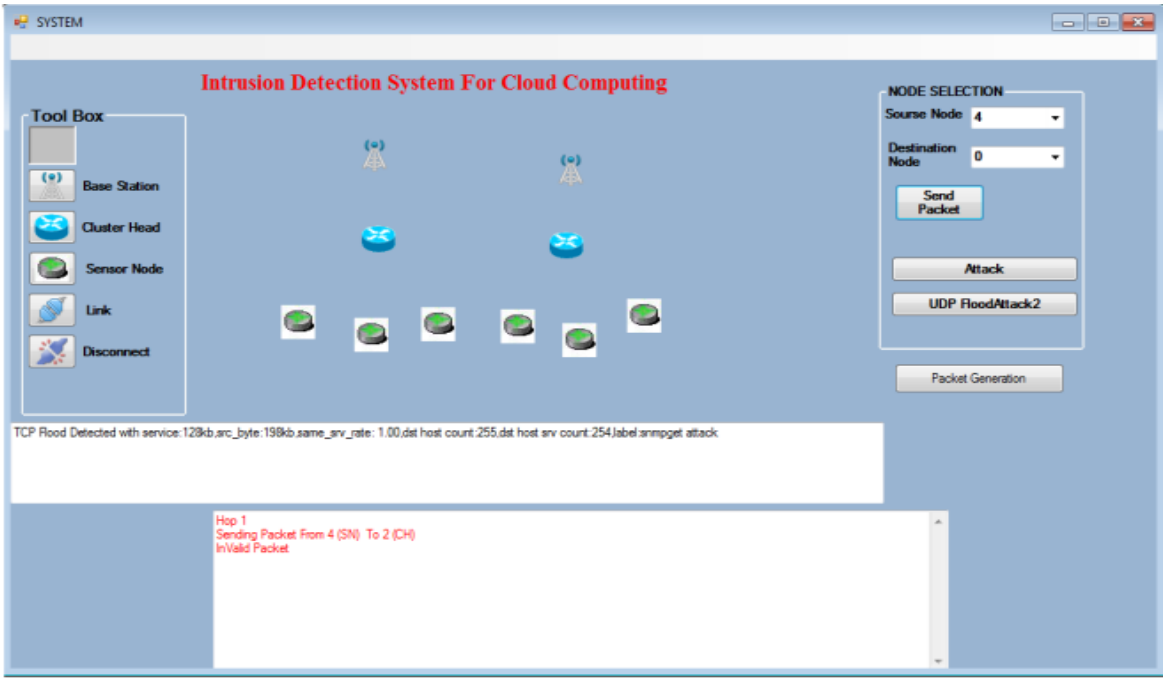

Figure (5)

In this case, monitoring and analyzing the event occurring in the wireless network in order to detect abnormal activities by applying genetic algorithm. The intrusion detection is defined as a mechanism for a packet in a network to detect the existence of inappropriate, incorrect or anomalous moving attackers. If the genetic algorithm found anomalous behaviors then the packet will be blocked. After filtering the invalid packet will be block and all the valid packet will reach to the destination.

V. FUTURE ENHANCEMENT

This will be implemented for unknown attack for the big data analysis. Since all the application will be internally connected so there will be need to provide for detection of unknown attack on the larger network. This model can be used with more security features can be implemented in it. In this manner, each feature is enhanced in order to improve the overall effectiveness of the system.

VI. CONCLUSION

Cloud computing is a "network of network" over the internet, therefore chances of intrusion is more with the erudition of intruder's attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For cloud computing, enormous network access rate, relinquishing the control of data and application to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this report, a multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user.

REFERENCES

[1] Mrs. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A.D.Gawande,"Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.

[2] Department of Computer Science & Application, Gyan Jyoti College, Siliguri Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology, Majitar, East Sikkim." USE OF GENETIC ALGORITHMS IN INTRUSION DETECTION SYSTEMS: AN ANALYSIS" International Journal of Applied Research and Studies (iJARS)ISSN: 2278-9480 Volume 2, Issue 8 (Aug 2013).

[3] S. N. Pawar Associate Professor (E &TC),Jawaharlal Nehru Engineering College, Aurangabad, MS, India. "INTRUSION DETECTION IN COMPUTER NETWORK USING GENETIC ALGORITHM APPROACH", International Journal of Advances in Engineering & Technology, May 2013.

[4] Monjur ahmed and mohammad ashraf hossain, senior lecturer,"CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD" daffodil institute of IT, Dhaka, Bangladesh, Vol.6, No.1, January 2014.

[5] Mohammad sazzadul hoque, md.abdul mukit and md.abu nasar bikas "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM",department of computer science and engg,shahjalal university of science and technology,sylhet,Bangladesh vol.4,NO-2 march12.

[6] Hamdan. O. Alanazi, rafidah Md Noor, B.B Zaidan, A.A Zaidan" INTRUSION DETECTION SYSTEM: OVERVIEW", journal of computing,volume 2,February 2010.

[7] Won Kim, sungkyunkwan university, suwon, s.korea"CLOUD COMPUTING: TODAY AND TOMORROW", vol.8, NO.1, January-february 2009.

[8] Kuyoro s.o. ,Awodele O, :CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES", Department of computer science, babcock university, llishan-remo,240001,Nigeria.

[9] Swapnil shinde,ashwini bangar,manali tawde, lecturer, dept of information technology"COMPARATIVE STUDY AND ANALYSIS OF IDS IMPLEMENTATION IN CLOUD COMPUTING ENVIRONMENT", RAIT, nerul.

[10] P. Praveen Kumar, K. Bhaskar naik, "A SURVAY ON CLOUD BASED INTRUSION DETECTION SYSTEM", Department of computer science sree Vidyanikethan engg college ,tirupati, INDIA.

[11] Pramod bide, Rajashree shedge, Department of computer engg,"COMPARATIVE STUDY AND ANALYSIS OF CLOUD INTRUSION DETECTION SYSTEM", Ramrao adik institute of technology/Mumbai universi