Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 6, June 2017, pg.425 – 429

SNORT based Intrusion Detection Model for Virtual Machine in Cloud Computing

Mr. Vijay Kumar S R[1], Mr. Rohit Kaliwal[2]

[1]Department of Studies in Computer Network Engineering, VTU Belagavi, India
[2]Assistant Professor Department of Studies in Computer Network Engineering, VTU Belagavi, India
[1] srvijaykumar07@gmail.com; [2] rohit.kaliwal@gmail.com

Abstract: Web services and cloud computing has evolved as an efficient medium for communication among the users, as well as between the machines. As cloud computing and the web services provide the quality data transfer, there are some concerns regarding the data security, as they operate over the internet data are prone to vulnerabilities. It is difficult to anticipate the intruder who tries to steal the data of the user. This works focuses on detecting the intruder and alerting the user about the same and also tries to recover the lost data and finally analysing the lost and recovered data packets using pie chart.
Keywords: cloud computing, web services, security, intruder detection, data recovery.

I. INTRODUCTION

As data is growing rapidly nowadays through many sources like social networking, banking and govt sectors etc, there should be an efficient method to store, manage and manipulate that huge amount of data, cloud computing does this job perfectly. To define cloud computing, "technology in which multiple users can own their data space in a single physical machine which is separated logically and can access to it according o their requirements". Using web service interface user can store any amount of data at any time in the cloud, and can preserve retrieve and restore their data.

It provides both hardware and software facility to the user. The user can choose any of these services and pay according to their use. In cloud technology, there is no need to install the huge data centre at the user premises instead it stores all the information in the remote place and user can access through the internet. A huge single physical machine is divided into partitions as virtual machines. Each virtual machine will be provided to one user, and users can use those VM as their data space. Users can scale up scale down their space according to their requirement and they should pay for what they consumed.

The core part of the technology is virtualization and this can be achieved by the hypervisor. Hypervisor is a virtualization software use to divide the physical machine logically. I.e. it allows service to host multiple operating systems to operate in a single computer simultaneously.

Cloud computing uses web services an integral part of it, through web services we can achieve the communication between the users as well as between the computers using internet. Particularly to transmit a typical pattern that is intended for the computer i.e. JSON and XML. It allows object oriented access to the database server. Using web services in cloud computing helps users to achieve an efficient data exchange and a reliable delivery of information. As cloud computing provides the services over the internet it has some security

hazards and that is the primary concern to be taken care of. Threats may target to the hypervisors, virtual machines, web services and web applications [1].

Restricted access to the confidential documents, susceptibility to the common controls and other related aspects. Intruder tries to exploit these susceptibilities to obtain the confidential data. Some of the threats are injecting of OS and SQL, manipulation of cookies, manipulation of hidden files, scanning the ports, injection of worms, of hypervisors, etc.As virtualization plays vital role in cloud computing i.e. dividing the physical machines into number of virtual machines, to host the different operating systems [2], as users are allowed to share the space in the physical machine, there are chances of security breaches i.e. users may try to know the data of the neighbouring users who shares the same physical machines. So this work focuses on detecting these types of intruders and alerting the users about the intruder. It also tries to recover the lost data, and analysing the lost and recovered data packets using pie chart

II. LITERATURE SURVEY

Many research work regarding the virtual machine security and web services security are proposed and still in progress. Studying of the normal and abnormal behaviour of the network traffic using software defined network, and also makes use of the SNORT, an efficient intrusion detection system. It can able to catch the virtual machine traffic and analysing the virtual machine network behaviours and have the control over the network system [1].

Approach towards the inter-virtual machine security vulnerabilities. Types of attacks like pretending as an authorized entity and tries to grab the data, peeping into the neighbour virtual machine i.e. sniffing attack, and other security issues. Provides a detailed solution to these issues like installing an efficient firewall, routing layer approach, and shared network layer in order to restrict the interface between the virtual machines [2].

Defining the cloud basics and the services offered by the technology. The security problems of the user's confidential data, detecting the attacks, providing suitable solutions to overcome. [3]

Addressing the security related issues in cloud computing because of the shared resources in a single physical machine. Proposing the Role-based Access Control (RBAC) method and the arrangement of strict information assurance and security. Besides, an anxiety tests utilizing disengagement benchmarking devices to assess the disconnection in holders in term of execution [4].

Addressing the various types in which the data is leaking and losing the integrity, the types of attacks and giving an effective ways to get through. Knowing the flow of data in the machine ranging by same virtual machines where same IP is being used by them [5]

Proposing the effective solution by the new method by keeping track of every movement and the changes in the environment and on that basis defining the suitable solution and making the system a reliable one. [6]

Approach towards discussing the capabilities of the detecting systems and flaws in the present methods. Providing a solution based on the method called RESTfull[7]

III.METHODOLOGY

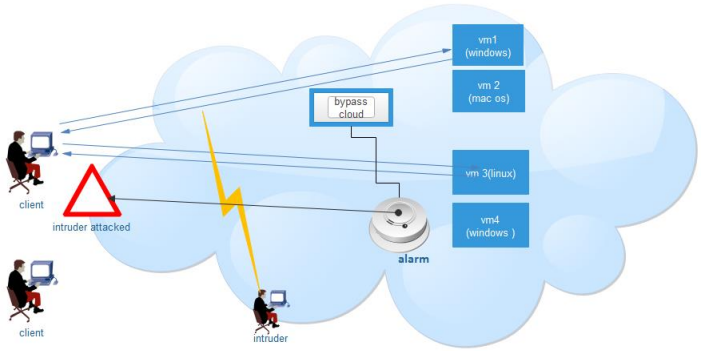

Figure 1: System Architecture

Fig 1 depicts the cloud environment in which there are two web services divided into two virtual machines each of which is installed with different operating systems. Clients can communicate to any of the virtual machines according to their need. As shown in fig, a client is exchanging the data between the two virtual

machines, during this process an intruder comes into the picture and tries to obtain the data. As soon as the intruder attacks, the cloud will be bypassed and information will be sent to the alarm to alert the user about the event. The user will come to know about the attack and ask for the permission to continue or to abort, after the user signal, the process will be continued, if the user does not allow, then the process will be terminated, or else it will be continued upon the user decision. After the attacker got the data of the user, next procedure will be to recover the lost data. When there is no intruder the process will take place normally, like, if client send any information to the data centre it will be stored directly into it, if there is any intruder comes to steal the data then it will ask for the user authentication, after the user signal the data will be stored in the data centre with the recovered data (data which was left after the attack along with the data lost by the attack)

IV. IMPLEMENTATION

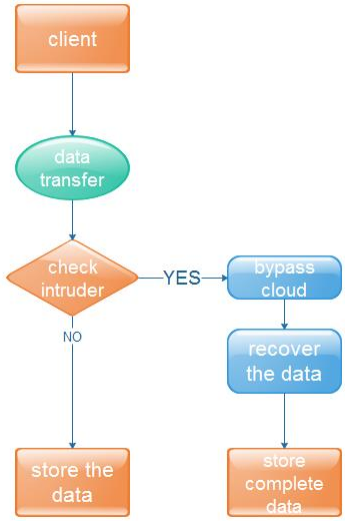

Fig 2 System Process

From the above figure the system process in which when a user need to send data to the data centre, at the beginning first it will check for the intruder or any other third party trying to get the data, if any of the intruder found then it will be indicated to the user, then the data is recovered from the attack and finally complete-data is stored in the data centre.

Snort: it is smart intrusion detection method in which it can able to detect the anomalies or the intruder activities in the cloud, if any of such event occurs it will alert the user about the attack and tries to recover the lost data.

Elements of snort:

Packet decoder: it takes the data packets from different sources and keeps it ready for the pre-processing or it ll send packets to the detecting system.

Pre-processors: these are the components which are used in snort in order to make modifications to the data packets, while the detection system check for the integrity of the data. It also performs the tasks of detecting model by detecting the intruders.

Detection engine: This is a core section. Helps in recognizing the flaws present in a data. In order to achieve this certain rules are followed. The guidelines are perused into inner information structures or chains where they are coordinated against all data packets. On the off chance that a bundle coordinates any run, proper move is made; generally the packet is dropped. Proper activities might be logging the packet or producing alarms.

Logging and Alerting System: based on what the location system finds inside a data packet, it might be utilized to log the movement or produce an alert. Logs are kept in basic content documents, tcpdump-style records or in any other shape. We can use command options and line choices to adjust the area of producing logs and alarms.

Output modules: these are capable of handling different tasks like maintaining and handling the data obtained which was generated using the snort.

V. EXPERIMENTAL RESULTS

Following pie charts shows the loss of data packets and the total packets, which are obtained in the process of data transferring between the user and the data centre. By this representation we can estimate the data loss during any communication in the virtual machines. The data loss will be dependent on the amount of data transfer between the user and the data centre.

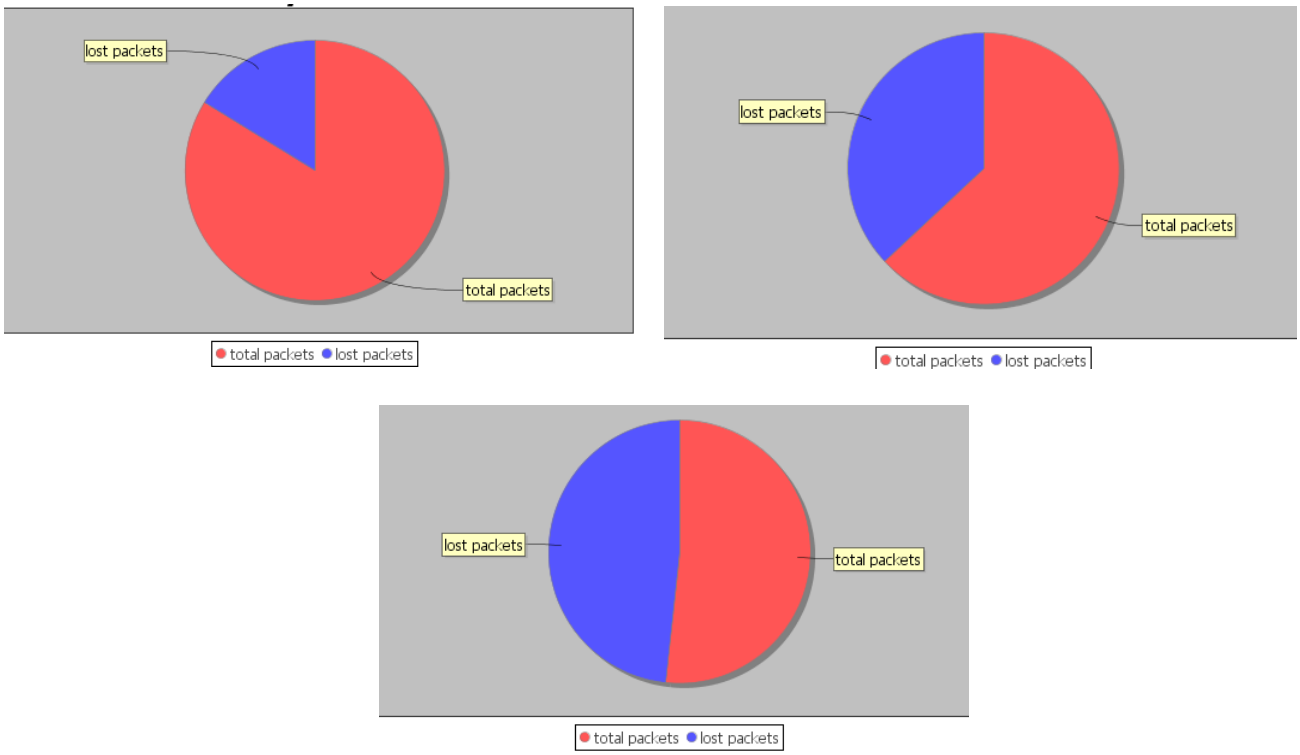

Fig 3 different data loss scenarios

VI. CONCLUSION

Cloud computing has emerged as an effective method of computing as well as providing different types of computing services by allowing the user to consume the computing resources according to their need and pay for what they used.

As the technology makes the work easier it is prone to some vulnerabilities like unauthorized access, data loss etc. This work proposes an efficient method to detect the intruder, trying to get the confidential data, alerting the user and even getting the information about the amount of data that has been attacked by the intruder. After the intruder attack data has been successfully delivered to the data centre without any loss and analyzed the lost data and recovered data using a pie chart.

The work can be extended to try in the real cloud environment to detect the intruder and to recover the data. Further study could be done in order to provide an efficient and trustworthy module to achieve the integrity and security of the data.

REFERENCES

[1] 1.Hanqian Wu, College of Software Engineering Southeast University Nanjing, China Hanqian@seu.edu.cn , 2.YiDing, Department of Electrical and Computer Engineering Purdue University Calumet Hammond, IN, USA dingy@calumet.purdue.edu, 3.Chuck Winer, Department of Computer Information Technology & Graphics, Purdue University Calumet Hammond, IN, USA Winer@calumet.purdue.edu, 4.Li Yao College of Software Engineering Southeast University Nanjing, China Yao.Li@seu.edu.cn .

[2] Xiaoming Ye, Xingshu Chen_, Haizhou Wang, Xuemei Zeng, Guolin Shao, Xueyuan Yin, and Chun XuAn "Anomalous Behaviour Detection Model in Cloud Computing" ISSNll1007-0214ll08/11llpp322–332Volume 21, Number 3, June 2016.

[3] Farhad Ahamed, Seyed Shahrestani, Bahman Javadi School of Computing, Engineering and Mathematics Western Sydney University Sydney, Australia, Security Aware and Energy-Efficient "Virtual Machine Consolidation in Cloud Computing Systems", 17368113@student.westernsydney.edu.au, s.shahrestani@westernsydney.edu.au, b.javadi@westernsydney.edu.au .
[4] Ibrahim Alobaidan, Michael Mackay, Posco Tso Department of computer sciences Liverpool John Moores University (LJMU) Liverpool, UK "Build trust in the cloud computing - Isolation in container based virtualisation" I.M.alobaidan@2012.jlmu.ac.uk, [M.I.Mackay], [P.Tso]@.ljmu.ac.uk.
[5]Udaya Tupakula Vijay Varadharajan Naveen Akku Information & Networked Systems Security Research, Department of ComputingFaculty of Science, Macquarie University, Sydney, Australia{udaya, vijay, naveen}@ics.mq.edu.au
[6]CloudWatcher: Network Security MonitoringUsing OpenFlow in Dynamic Cloud Networks(or: How to Provide Security Monitoring as a Service inClouds?)Seungwon ShinSUCCESS LabTexas A&M UniversityEmail: seungwon.shin@neo.tamu.eduGuofei GuSUCCESS LabTexas A&M UniversityEmail: guofei@cse.tamu.edu
[7] RESTful Web Services for High Speed Intrusion Detection SystemsMohsen RouachedCollege of Computers and Information TechnologyInformation Technology DepartmentTaif UniversityTaif, Saudi Arabiam.rouached@tu.edu.saHassen SallayDeanship of Information TechnologyInformation Security DepartmentAl Imam Mohammad Ibn Saud Islamic University (IMSIU)Riyadh, Saudi Arabiahmsallay@imamu.edu.sa

