ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
*Published By:* **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 438-445

# Hybrid Intrusion Detection System for Private Cloud & Public Cloud

**RIDDHI GAUR and UMA KUMARI**

Dept of CSE Mody University of Science and Technology Lakshmangarh, India

http://dx.doi.org/10.13005/ojcst/10.02.26

(Received: May 05, 2017; Accepted: May 12, 2017)

**ABSTRACT**

Internet based applications and data storage services can be easily acquired by the end users by the permission of Cloud computing. Providing security to the cloud computing environment has become important issue with the increased demand of cloud computing. Other than the traditional security methods, additional methods like control access, confidentiality, firewalls and user authentication are required in order to provide security to the cloud computing environment. One of the needful components in terms of cloud security is Intrusion Detection System (IDS). To detect various attacks on cloud, Intrusion Detection System (IDS) is the most commonly used mechanism. This paper discusses about the intrusion detection and different intrusion detection techniques namely anomaly based techniques and signature based techniques.

**Keywords:** cloud computing; intrusion detection system; anomaly based intrusion detection system; misuse based intrusion detection system.

## INTRODUCTION

Cloud computing is an emerging technology in the IT sector. It is a collection of sources that are conveyed on demand over the network for enabling resource sharing in terms of manageable computing services and scalability. By the help of third party, cloud basically provides services to other organizations. The third party provides resources and services on rent and users pay per usage. The users can save large amount of cost as the users does not need to buy any resources or software or any infrastructure. This provides a great flexibility to move from one service to another service and saves lot of money.

Recently world of computation has emerged a lot and world is moving towards virtual centralization i.e. Cloud computing[1]. Cloud services are being used very frequently by the users so the users are unaware of the security concerns in a cloud environment. Cloud computing is more vulnerable to security risks as it is distributed in nature and it supports multiple users and multiple domain platform.

An Intrusion detection system examines all internal and external network activities or attacks and identifies suspicious design that may point out the system attack or a network from someone attempting to break into the security or compromise a system[2]. The cloud computing uses the web as the communication media. Every user can easily accessed the cloud computing services without any legal permission, so the cloud computing gets easily frightened by various attacks. Due to the distributed nature of cloud computing, cloud computing environments are easy targets for invaders looking for possible susceptibility to exploit.

In this paper Section 2 describes cloud computing service models. Section 3 tells about the intrusion detection system.

**intrusion Detection System**

Intrusion detection system (IDS) is an extremely important of protective determination to preserve the computer system and network opposite various attacks. The main motive of IDS is to create a proper reply and detect the several attacks. It is described as procedures which are used to reply and reveal to the intrusion projects for destructive network or host. In addition, the IDS can find the malicious activities in a network and also be described as a protection system. To discover the activities that may compromise with the system security and possibly blocking them is the only solution. The key attribute of intrusion detection system is to create the alerts so that the administrators can be informed to prevent the eliminated bond and its capability to provide the vision of abnormal project. Intrusion detection tools can differentiate the insider attacks that are derived into the inner side of the organization and the external attacks which occur outside the organization.

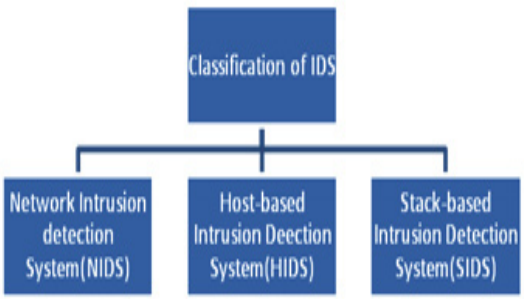


**Fig. 1: Classification of IDS**

The problems of intrusion detection system provide awareness for informing about the occasion if an intrusion has been discovered. These alarms are based on right alarms when actual intrusion takes place and when wrong detection of the system takes place false alarms are created. After this, intrusion detection system or controller itself takes certain steps corresponding to administration strategies. If rate of detection is greater and rate of false positive is low at intrusion detection system then capability of the intrusion detection system is good. On other hand if the detection rate is smaller and false positive rate is high at intrusion detection system then capability of the intrusion detection system is bad. Few security issues related to cloud are data breaches, compromised credentials and broken authentication, hacked interfaces and application program interfaces, account hijacking, secure service management, management of trust, shared technology, exploited system vulnerabilities, administration management, permanent data loss, data protection and security management[4].

**Classification of IDS**

The intrusion detection system is broadly classified into three main types

**Network Intrusion Detection system (NIDS)**

The main target of this intrusion detection system is on the computer network and not on the host system. The system finds out the attacks through assembling and then observing the packets of network. Representing the network traffic packets such as TCP; UDP, NIDS make efforts to detect unapproved permission to a computer network and examine the content opposite to the set of rules. Few examples are: Denial-of-Service (DoS) attacks, Shadow, Snort, Sax2, Dragon, Real Secure, Eavesdropping, and Man in the middle attack. NIDS are placed at different points in the network which comprises of a set of single-purpose sensors. Sensors send survey of attacks to the consolidate comfort and inspect network traffic. Network intrusion detection system (NIDS) has a very tiny effect on the performance of the network through implementation. Useful characteristics of network intrusion detection system are that it should

be able to detect known and unknown attacks and also capable of discovering intrusions at each component like front end; back end..

**Host-based Intrusion Detection System (HIDS)**

In this type of intrusion detection method the detection of intrusion is performed on one of the host machine. To discover any type of change or modification of the system the integrity of the data is verified which is collected by the host system. This is possible by examining the system calls for detecting the intrusions and by using hashing tools or system logs.

HIDS involves operative or software elements, which detects the effective performance and situation of the computer systems. Host-based intrusion detection system software runs on the router; server; switch or network mechanisms. Representative model can run on the same host or has to report to the console. Examples are: Overflow buffer, Root kit, string format, etc. The software generates system log of files in the structure of origin of the information. By looking at communication traffic the host based inspects the uprightness of system files to keep an observe on suspicious procedures. Host-based intrusion detection system (HIDS) does not produce good real time acknowledgement.

**Stack-based Intrusion Detection System (SIDS)**

This is the newest intrusion detection system IDS[5] technology and a progression of intrusion detection system (IDS) that changes from host to host. SIDS works in non-promiscuous way

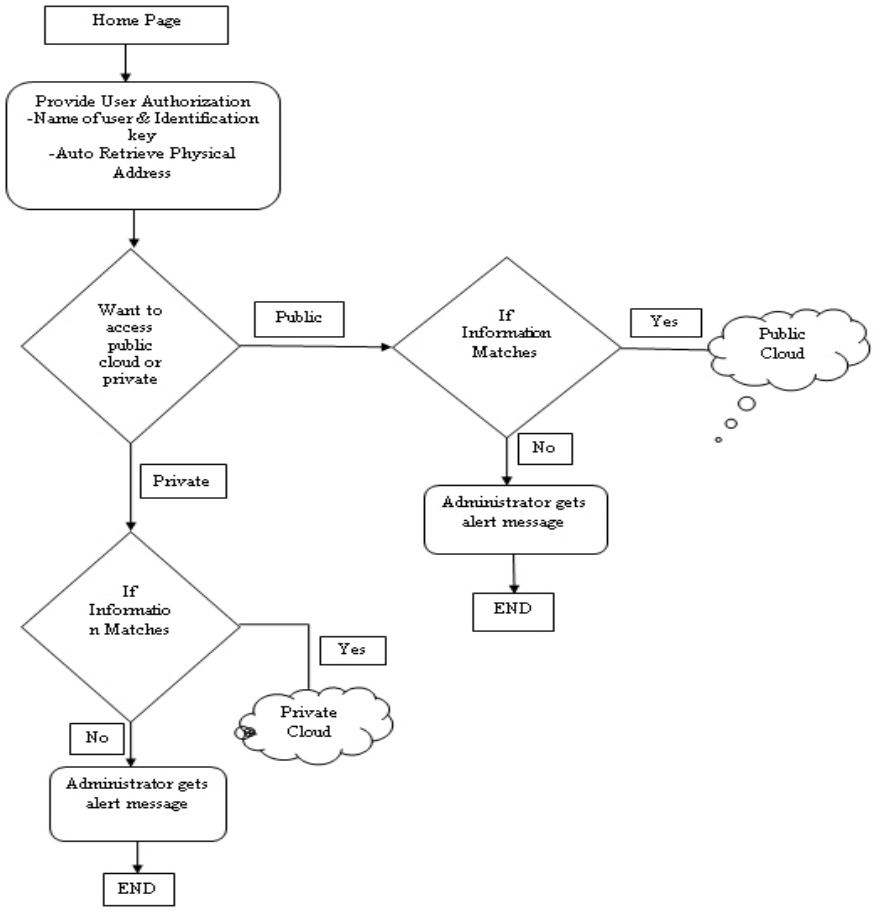


**Fig. 2: Flow chart of HIDS Method**

and works combining closely with the TCP or IP stack authorizing packets to be examined as they negotiate their way up the OSI Layer

**Table 1: Performance of IDS for 50 Users for private cloud**

| LABEL | Sample | Response Time (sec) | Throughput | Data Transfer |
|---|---|---|---|---|
| gmail | 50 | 2.127 | 30.023 | 54.94 |
| mody university | 50 | 0.609 | 30.504 | 9.47 |
| TOTAL | 100 | 1.368 | 30.263 | 32.20 |

**Table 2: Performance of IDS for 100 users for private cloud**

| LABEL | Sample | Response Time(sec) | Throughput | Data Transfer |
|---|---|---|---|---|
| gmail | 100 | 2.092 | 59.631 | 98.47 |
| mody university | 100 | 0.577 | 60.374 | 20.98 |
| TOTAL | 200 | 1.334 | 60.00 | 59.72 |

**Table 3: Performance of IDS for 50 users for public cloud**

| LABEL | Sample | Response Time (sec) | Throughput | Data Transfer |
|---|---|---|---|---|
| google | 50 | 1.812 | 30.165 | 41.44 |
| ibm | 50 | 1.078 | 30.307 | 28.38 |
| TOTAL | 100 | 1.445 | 30.236 | 34.91 |

**Table 4: Performance of IDS for 100 Users for public cloud**

| LABEL | Sample | Response Time (sec) | Throughput | Data Transfer |
|---|---|---|---|---|
| google | 100 | 1.459 | 59.707 | 84.07 |
| ibm | 100 | 1.129 | 60.047 | 54.24 |
| TOTAL | 200 | 1.294 | 59.877 | 69.155 |

**Detection Techniques in IDS**

**Signature/Misuse based detection**

This is the method used for detection of attack that is affected by the system. This method utilizes signatures specifically known patterns of unapproved performance to speculate and discover successive indistinguishable attempts[6]. This method processes a low false alarm and is ultimately valid for known attacks. One can adopt go across a broader range of unknown attacks with the help of this procedure. One important benefit is that signatures can be understood and easily generated only if the network performance is known. The disadvantage of this method is that to detect a new attack a set of signature must be endlessly improved otherwise it cannot discover any narrative attacks. And it can only discover intrusion that matches with a prebuilt design. When the user starts using advanced technologies like payload encoders and encrypted information channels[7], misuse/signature based detection does not function very well. As the number of new attacks increases, the efficiency of signature/misuse based systems decreases due to the production of a signature for each new attack.

**Anomaly based detection**

This type of approach is considered as an attack[8] and also evolved in order to flaunt the patterns which are not similar to the normal activities. It works for the concept that each attack is dissimilar from daily activity and can be discovered by systems that identifies the differences because anomaly detectors are depicted to detect behavioral abnormal patterns on a network or host.

Anomaly detectors produce a record of profile information as usual information,

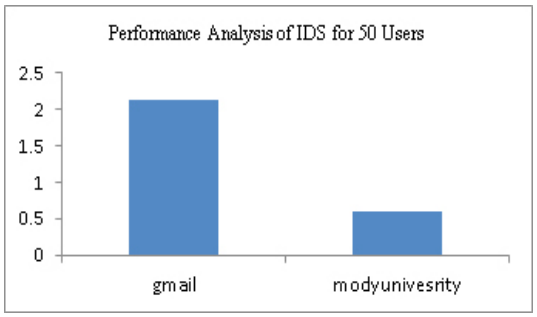


**Fig. 3: Performance of IDS for 50 users for Private cloud**

illustrating normal performance. It produces alarm by automatically discovering any inconsistency of it and has the capability to discover new errors. The advantage of anomaly based detection is that without altering existing ones[9], we can attach new rules. Many procedures and measures are used in anomaly detection including: Genetic methods, Rule based measures, Threshold detection, Networks immune system framework, Statistical analysis and Neural[10]. Anomaly based detection has the capacity to discover narrative attacks. But this procedure creates many wrong alarms by delaying the time utilized for completion of the analysis to acquire updates and accurate the comprehensive profiles of performance [11]. Because of which it requires a large deposit of training information with records of the network environment system.

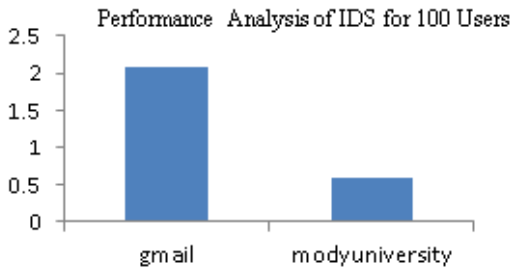


**Fig. 4: Performance of IDS for 100 users for Private cloud**

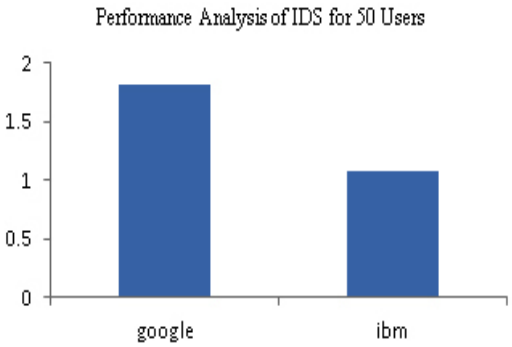


**Fig. 5: Performance of IDS for 50 users for Public cloud**

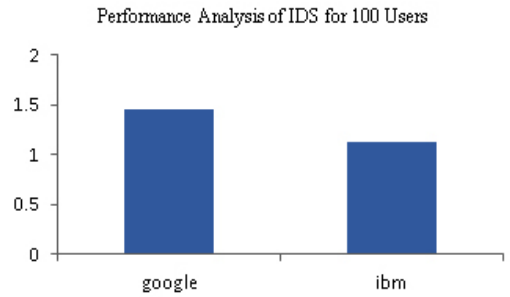


**Fig. 6: Performance of IDS for 100 users for Public cloud**

**Hybrid intrusion detection method**

Hybrid Intrusion Detection Method (HIDM) can be designed for hybrid cloud. HIDM has three phases: Registration stage, Signature analysis stage, Anomaly analysis stage and Signature analysis stage.

Hybrid intrusion detection method consists of the input which comprises of the arriving request and the output flaunts all the request details and highlights the unusual request. The method consists of few steps which begin with the start procedure and then the number of cloud users will be computed for all the n cloud users. After the calculation of users, implementation and computerization of the registration stage, anomaly analysis and signature analysis stage will begin. And in the last the procedure ends.

Now after the first step, registration stage starts. Registration stage consists of the input which contains identification key, username and physical address and the output comprises of keeping records of authorized user. The registration stage begins with the start procedure for all the n users of the cloud. And then acquire correct email-id and identification key. Then auto retrieve physical address of the system. After auto fetching the physical address, check if the value of identification key, email-id and physical address is correct or not. If the values are correct then the certification is done successfully. If the values are not correct then the registration process will get stop and it will aware

**Table 5: Summarized Performance Evaluation**

| S. No | Total no. of Sample | Type of Cloud | Average Response Time (sec) | Ave. Throughput | Average Data Transfer |
|---|---|---|---|---|---|
| 1. | 100 | Private | 1.368 | 30.263 | 32.30 |
| 2. | 100 | Public | 1.445 | 30.236 | 34.91 |

the executive of the network for abnormal activity. And in the last the procedure ends.

Signature analysis stage(SAS) consists of the input i.e. identification key, email-id and physical address and for the output inspect and exhibit the request details and highlight the unusual request. SAS method begins with the start procedure. Then we will examine all the arriving requests. Read the identification key, physical address, email-id, port number and protocol of the arriving request. Then check the email-id, identification key and physical address is correct or not, if the values are not correct then the incoming request may be an intrusion so, highlight the request and aware the executive. Also if the port number and protocol is not well known, then the appeal may be an intrusion and highlight the request and aware the executive. If the signature analysis stage is successful then move to the next phase i.e. anomaly analysis stage else alert the head to monitor the activities of the network. And the signature analysis stage method ends.

Anomaly check phase begins with the input as the incoming request and the output flaunts the bandwidth of the request. This algorithm begins with the start procedure. For all the arriving appeals settle the threshold value of the bandwidth and the request speed until the value of i is 10. Examine the appeal speed, appeal bandwidth and flaunt it. The appeal may be an intrusion if the speed of the appeal is equal or less than the threshold cost of desirable speed. Highlight the appeal displayed or investigate the bandwidth of the appeal. The appeal may be an intrusion if the bandwidth cost is greater than the threshold of the bandwidth and then highlight the displayed appeal. Detect average cost of the bandwidth and appealed speed; if the average appealed speed is more than the appealed threshold cost then notify threshold cost with average cost of the appealed speed else shift to the bandwidth principle. Notify the threshold cost with average cost of bandwidth if the average bandwidth is smaller than the threshold of the bandwidth. Repeat for all the arriving appeals. And in last anomaly analysis stage method ends.

**Design of hids method**

The above proposed method is designed considering the cloud's nature, the characteristics of the cloud and the Intrusion detection characteristics for the cloud based environment. The above figure gives an overall vision about the flow of method and execution of Hybrid Intrusion Detection method in a cloud environment. All the user information will get stored by the head of the cloud in the data base. After the registration process there will be two options for every user: want to access public cloud method or private cloud method.

Users who want to access public cloud method will select public cloud method. If the user logins, the arriving login will be examined across various principle which are prebuilt by the executive after the registration phase. Intrusion awareness will be sent to the executive if the appeal differs from the prebuilt information else the executive will grant permission to the user to use the public cloud method. The same will happen with the users who choose private cloud method. Intrusion awareness will be sent to the executive if the request differs from the prebuilt information else the admin will grant permission to use the private cloud method.

**Performance Evaluation**

Using Open Source Performance testing tool JMeter, the performance of the Intrusion Detection System can be checked The testing of the intrusion detection system has been performed using the following algorithm in which the input consists of certain websites which belong to the private and public cloud and the output comprises of the response time, throughput and amount of data transferred. We will start the algorithm and then load the user thread. Specify the number of users going to use the system and then initialize the samplers for particular websites and the listeners for the output. Execute the listeners and check whether all the listeners are executed correctly otherwise perform the procedure again. And at last the algorithm will end.

## RESULTS

Using JMeter, intrusion detection system has been executed with 50 users and 100 users for private cloud and public cloud. The performance of the system is calculated using the terms such as throughput, response time and data transferred. Median and average are also produced by the

**Table 6: Summarized Performance Evaluation**

| S. No | Total no. of Sample | Type of Cloud | Average Response Time (sec) | Ave. Throughput | Average Data Transfer |
|---|---|---|---|---|---|
| 1. | 200 | Private | 1.334 | 60.00 | 59.72 |
| 2. | 200 | Public | 1.294 | 59.877 | 69.155 |

JMeter. JMeter produces the response time in Milliseconds which are converted into seconds in all following tables.

The figure below gives the graphical representation of the response time. Since the graph which is generated by the JMeter have readability issues, the values given in the table 2-5 are interpretated in the form of graph in which the x-axis values indicate the sample value and the unit is count and the y-axis values indicate the response time and the unit is in seconds.

**The results which are obtained from table 5 & table 6 are as follows:-**

When the number of users gets increased in both the clouds, the average value of throughput is still constant which indicates that the algorithm is efficient in terms of time complexity.

Even if the number of users get increased in both the clouds, the average value of the amount of data transferred is nearby same which indicates that the algorithm is efficient in terms of the amount of data consumed.

**Future Scope**

The algorithm proposed in this paper can also be executed in any other cloud deployment model. The algorithm can also improve its performance by increasing the total users. By modifying the values which are based on the limitation of time, the performance of the algorithm gets better. The concept of fuzzy can also be added in the future work to increase the efficiency of the algorithm. Using artificial intelligence, the algorithm can work in another direction for research for detection of attacks in a cloud environment.

## CONCLUSION

Cloud Computing has given rise to a new services paradigm to the internet technology. Chances of intrusion are more because cloud computing is distributed in nature. Detecting various procedures of intrusion detection and prevention systems have reveal that either using anomaly or misuse based procedures all alone will not provide determined security attributes. Hence, a hybrid mechanism can be executed to enhance the detection rate. The proposed method can be executed in other cloud deployment model. By joining much more principle the effectiveness of the method can be enhanced to discover an Intrusion in a network. By improving the values based upon the limitation of time the implementation of the method can be enhanced. If the counting of users gets enlarged, the performance of the proposed method will hold well. The efficiency of the proposed algorithm in terms of time complexity and amount of data used is good. Graphical representation was carried out for response time as it is the key factor of our research. In our future work, performance analysis will be performed on other parameters such as the amount of data transferred and the throughput.

## REFERENCES

1. S.V. Narwane and S.L Vaikol, “Intrusion Detection System in Cloud Computing Environment”, International Conference on Advances in Communication and Computing Technologies (ICACACT), 2012.
2. Deris Stiawan, Abdul Hanan Abdullah and Mohd. Yazid Idris, “Characterizing Network Intrusion Prevention System”, *International Journal of Computer Applications*, Vol.**14**, No.1, 2011.
3. Eugene Gorelik, “Cloud Computing Models”, Massachusetts Institute of Technology Cambridge, MA 02142, 2013-01.
4. Pradeep Kumar Tiwari and Dr. Bharat

Mishra," Cloud Computing Security Issues, Challenges and Solutions", International Journal of Emerging Technology and Advanced Engineeering, ISSN 2250-2459, Volume **2**, Issue 8, August 2012.

5. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel and Muttukrishnan Rajaranjan," A survey of Intrusion detection techniques in cloud", *Journal of Network and Computer Applications*, pp.42-57, 2013.
6. AhmedPatel, Mona Taghavi, Kaveh Bakhtiyari and Joaquim Celestino junior, "An intrusion detection and prevention system in cloud computing: A systematic review", *Journal of Network and Computer Applications*, Volume **36**, Issue 1, pp.25-41, 2013.
7. V.Jyothsna, V.V. Rama Prasad and K Munivara Prasad, "A Review of Anomaly Based Intrusion Detection System, *International Journal of Computer Applications*, Vol.**28**-No.7, 2011.
8. M.M.M.Hassan," Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic", International Journal of Distributed and Parallel Systems, Vol.**4**, No.2, pp.35-47, 2013.
9. Ms. Parag K Shelke, Ms. Sneha Sontakke and Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research,Vol.1,ISSN 2277-8616, 2012.
10. Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah and Al-Sakib khan Pathan,"IDPS: An integrated Intrusion Handling Model for Cloud Computing Environment, International Journal of Computing and Information Technology (IJCIT), 2012.
11. Ms. Parag K Shelke, Ms. Sneha Sontakke and Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research,Vol.1,ISSN 2277-8616, 2012.