Entropy Variation and J48 Algorithm based Intrusion Detection System for Cloud Computing

Sreeja Nair
Prof. CSE Department, OIST Bhopal

Nupur Gautam
Student, OIST Bhopal

ABSTRACT
Now Cloud Computing has achieved formidable impetus where IT infrastructures and applications are provided as service to end users. It provides shared pool of resources in addition with Data storage, computer processing power and specialized corporate and user applications. Users can access Cloud services any time anywhere and store large amount of data from anywhere, due to increases the popularity of Cloud computing there is risk of Security. Data which is stored on cloud may be vulnerable which is easy for attackers to compromise the virtual machines as zombies and explore these vulnerabilities in cloud system. Because when we move data or information in cloud we do not have any control on that data which can be handling by third party. Hence, there is the vital requirement of more security measures to protect cloud. In this paper we propose an Intrusion detection system which is based on Entropy variation and J48 Decision tree algorithm through which we can detect or prevent vulnerable virtual machines, Data center and Host from being compromised in the cloud also we can protect data and applications in Cloud like wide area network traffic. This proposed solution results gives more accuracy for attack detection and low false alarm rate. For simulation we use Cloud Sim (version 3.1) and used KDDCUP '99 Dataset to evaluate rules and testing datasets to detect intrusion.

General Terms
Cloud Computing, Security, Decision tree algorithm, Traceback Method.

Keywords
Attacks and Security issues in Cloud, Entropy Variation, J48 Algorithm, KDDCUP'99 dataset, Cloud Sim.

1. INTRODUCTION
Recent survey about the Cloud Computing shows that many user or Organizations are immigrating to the cloud, because they provide shared pool of resources such as storage for data, computer processing power and many more in a cost effective manner. Despite all the advantages of cloud they are afraid to adopt cloud services, because there is some critical issue which is Security. There are a lot of data stored by different user from different user which can be vulnerable in cloud [1]. Survey of Cloud Security Alliance shows that among all security issues in cloud computing where attackers can compromise cloud resources and exploit vulnerabilities. Users can request a cloud for services, applications, solutions and might store a large amount of data from completely different location, however due to day by day increases the uses of cloud computing services there is even growing risk of Security. Cloud computing accommodates services through the internet on the basis of pay per usage model and it is the combination of distributing Computing, utility Computing and Grid Computing. Organizations use the cloud in a variety of service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, and hybrid). So that, Not only Cloud users but also the attackers share infrastructure or computing resources which connected through same switch, share same data storage and file systems Security is one of the vital issues which decrease the epidemic evolution of cloud. Security issues such as unauthorized server, data leakage, loss of user entity id and password and network security threats (DNS attack and sniffer attack). To detect and monitor the suspicious activity in network, Intrusion Detection System (IDS) and firewall are widely used [2]. Yet, there are two major problems in IDS implementation is the false alarms and the large volume of raw alerts. Intrusion detection technology is a fundamental mechanism for network security can monitor and detect suspicious activities like unauthorized network usages or abnormal conditions without affecting network performance, and then counter such phenomena. In this research paper we tend to propose a new Intrusion detection system which incorporates traceback method entropy variation which is different from the other traceback method like packet marking and Decision tree J48 classification algorithm which is more accurate than other techniques for attack detection. This proposed system can prevent vulnerable virtual machines, Data center and Host being compromised by the attacker in the cloud and also it can manage wide area network access traffic like in cloud. This proposed solution can be deployed in an Iaas cloud networking system. Cloud Sim (version 3.1) used for simulation and KDDCUP '99 Dataset used to evaluate rules and testing datasets to detect intrusion.

1.1 Security Issues in Cloud Computing
Cloud computing security is a combination of computer security, network security and information security. Without forehand investment it provide new implemented business model with modernized IT services for companies and end users. Despite these benefits achieved from the Cloud Computing the organizations are slow in accepting it because of security problems and challenges related to it. Means there is uneasiness for cloud users to store data in cloud because user data can be in control of another party. Cloud providers are using IP address to diagnose the computer systems and Virtual machines in the internet. So, it is easy for malicious user can commence attack on cloud infrastructure like it can search physical servers through which several users are connected and implement Virtual machine which is shared by users. Another security concern is Virtualization which is important part of the Cloud computing, it's very critical to preserve security texture where vulnerability or configurations errors are easily rendered.

Today there are a lot of attacks in the IT world. Cloud services not only used by legitimate users but also used by malicious users or attackers. In table 1.1, we summarize the some attacks which can affect the Security system of Cloud:

Table 1. Attacks in Cloud Computing

Types of attacks	Description
Session Hijacking	In session hijacking, through the user's session id attackers regain the information locate in computer system.
Virtual Machine Escape	It is an exploit in which the attacker runs code on a VM to gain access on the host operating systems.
Insecure Cryptographic storage	In this case attackers can regain the insecurely reserved data (like username, password etc.) with a small effort.
SQL Injection	This technique used to exploit web sites by altering backend SQL statements through manipulating application input [16]. The attacker steals the data from database and modifies it.
Denial of Service Attacks	It makes the resources unavailable for the users. In the cloud system the attacker attack through simply sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly.
Neptune attack	It is a kind of Denial of Service attack. During this attack, attacker sends session establishment packet with forged source IP address. The Victim machine the uses its resources and waits for session conformation. During the time slice, victim machine becomes unavailable to legitimate traffic.
Smurf attack	This is the form of DoS packet flood attack and Directed Distributed network flooding attack initiated by sending ICMP ECHO REQUEST Packets (Ping) to a broadcast address with the spoofed source address of the target. The target is then flooded with ECHO REPLY packets from every host on the broadcast address. [17].
Man-in-middle attack	If two parties are communicating each other and SSL is not properly installed then all the Data communication between two parties can be hack by the middle party.
Port Scanning	Port 80 (HTTP) continually open that is used for providing the web services to the user. Other ports such as 21 (FTP) etc. are not opened all the time.
Nmap attacks	It is a probe attack in which the hacker scans a machine or a networking device in order to determine vulnerabilities that may later exploited then compromise the system.

The rest of the paper is organized as follows: Section 2 presents the related work, Section 3 describes about problem statement, Section 4 describes proposed method, and description of proposed methodology which used in proposed system defines in section 5. Algorithm which is provided for proposed method is defines in section 6 and implementation, Evaluation of proposed system in terms of network performance and security describes in Section 7. Finally, section 8 describes the conclusion of paper and future work.

2. RELATED WORKS

In this section, we present literatures survey of several papers which describes different techniques used to protect Cloud and also define paper which is based on traceback method and decision tree algorithm.

[1]. The work by Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee and Dijiang Huang [3] focuses on the detection of compromised virtual machines then prevent Zombie VMs. Their proposed approach NICE (Network intrusion detection and countermeasure selection in virtual network systems) is based on attack graph analytical model which employs a reconfigurable virtual networking approach to detect and counter the compromise VMs. It also captures and inspects suspicious cloud traffic without interrupting users' applications and cloud services. Through the programmable network approaches, NICE can improve the flexibility to VM exploitation attack without interrupting existing normal cloud services. NICE elevate the implementation on cloud servers to minimize resource consumption.

[2]. Sandeep K. Sood proposed framework [4] which is a combination of different technique and designated procedures (such as SSL (Secure Socket Layer), 128 bit or 256 bit encryption, MAC (Message Authentication Code), searchable encryption, MAC (Message Authentication Code), Searchable encryption and Division method) which can protect data, check integrity and authentication of data in the Cloud from beginning to end. Also they classify data on the basis of Cryptographic parameters (like Confidentiality, Availability and Integrity).

[3]. Mr. Prashant Rewagad, Ms.Yogita Pawar [5] takes the combination of authentication technique (Digital signature) and key exchange algorithm (Diffe Hellman key exchange) integrate with encryption algorithm (AES(Advanced encryption standard algorithm)) because they ensures all three protection scheme of authentication ,data security and verification at the same time. Through this three way mechanism it difficult for hackers to crack the security system. In this proposed architecture Firstly Diffie Hellman algorithm is used to generate keys for key exchange step, then digital signature is used for authentication, thereafter AES encryption algorithm is used to encrypt or decrypt user's data file.

[4]. In this survey paper [6], Helen Sara George and Mrs.Jeno Lovesum describes different encryptions methods which are used to ensure security in cloud storage system and compare them. Result evaluation show that the proxy re-encryption methods are more substantial and convenient also it can reduce Network traffic.

[5]. In this research paper, Farzad Sabahi [7] summarize reliability, accessibility and security which given as RAS issues for cloud computing, describe several traditional solutions and countermeasures which provide security in cloud. In migration, accessible technique should be predicted

adjustment time and take a look at avoid cloud nodes overload by some procedure such as partitioning and fragment and moving data in smaller pieces of data and preserving the flexibility to run transactions whereas movement occurs.

[6]. Proposed framework [8] includes Digital Signature and RSA asymmetric algorithm to protect data in cloud environment. To provide authentication they use Digital signature by using hashing algorithm and provide encryption through RSA algorithm.

[7]. This Proposed method [9] based on hybrid statistical technique which uses data mining and Detection Tree Classification. For detection Authors include statistical analysis of both attack and normal traffics which is based on KDD Cup 99 which results can be employed to reduce misclassification of false positive and define differences between them.

[8]. This research paper [10] include systematic review of intrusion detection and prevention system which is used to provide security in cloud computing. Ahmed Patel, MonaTaghavi, and KavehBakhtiyari describe various IDPSs and alarm management techniques by using classification and evaluate them to detect and prevent intrusions in Cloud. After results they proposed CIDPS (Cloud Based Intrusion Detection and Prevention System) with the help of four important characteristics (Autonomic computing, Ontology, Risk management, fuzzy theory) of the IDPS and cloud computing systems.

[9]. Proposed system [11] can detect DOS attack on the basis of features set by using NSL KDD dataset. The result analysis shows that performance of IDS can be improved when more feature set is used for classification on the basis of classification accuracy and less classification time. By using composition of classification accuracy and time IDS can be made more efficient and reliable.

[10]. Shui Yu, Wanlei Zhou, Robin Doss and Weija Jia [12] provide a Novel traceback method called entropy variation based on information theoretical parameters which is used for detection of DDoS attack. Their experiment results show that traceback is possible in approx 20 seconds in any large area network which consist of attack like zombies. They used packet number distributions of packet flows and calculate entropy to compare between legitimate flows and attackers packet flows.

[11]. Sharmila Wagh and their group members [12] proposed a semi-supervised machine learning approach to improve performance and reduce false alarm rate of the pattern based IDS through KDD CUP99 dataset and J48 algorithm. This proposed approach has ability to improve performance of any given base classifier in the presence of unlabeled samples.

3. PROBLEM STATEMENT

Cloud computing provide flexible and scalable computing resources which is shared among the numerous users which can be legitimate user or attacker. There is lot of security issues like data loss or Zombie like DDoS attack which are critical to identify in large scale network like cloud. Our goal is to preserve the Cloud Environment from inside or outside attacks which is studied from different security models obtainable for Cloud Computing. Its effects are elaborate by stating however these attacks disturb the performance of cloud model and show unsafty of data that is stored in cloud.

4. PROPOSED SYSTEM

We tend to proposed solution to protect cloud from inside or outside attacks like distributed denial of service attacks which are critical to identify in cloud system. This proposed solution utilizes the concept of traceback method entropy variations and J48 decision tree classification algorithm. It works as Distributed intrusion detection system which provides functionality of Host based and network based intrusion detection systems. This system can be deployed on any system in cloud environment as software. For performance evaluation and simulation we used CloudSim (version 3.0). When any user wants to store data in datacenters or virtual machines within cloud. First it passes through the broker where intrusions detect through entropy variations then encrypt by using AES encryption algorithm then send to data centers or virtual machines. After that datacenter detect the intrusion on the basis of J48 classifier. For classification in J48 algorithm used KDD CUP 99 Datasets. Figure shows proposed system of our research work.

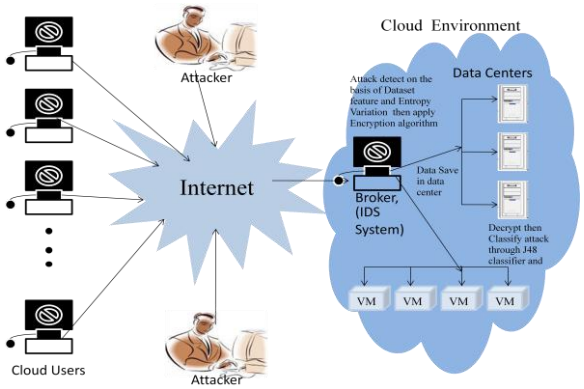

Fig.1 Cloud Networking Model

5. METHODOLOGY USED IN PROPOSED SYSTEM

5.1 Entropy Variation

Entropy is the information theoretic concept which is used to measure the randomness of variable which is random and in network it can be used for data flow. The range of entropy is 0 to log n [14]. Entropy variation can be used to detect attack in network through measures the uncertainty of packet flow.

Entropy according to Shannon is:

$$H = -\Sigma\, Pi \log2\,(Pi)$$

Where *pi* - probability

$$Pi = \frac{\text{Number of analyzed Packets received}}{\text{Total number of packets}}$$

Compare to other traceback method like DPM (Deterministic Packet marking) and PPM (Probabilistic Packet marking), entropy variations has a lot of advantages. Scalability of entropy variation is very high means over DPM which can handle 2^17-2^25 computers for single packet marking. Operational workload is very low because it counts the packets for each flow where this workload for DPM and PPM is very high due to it digest and Mark packets with probability P (about 1M packets/second). Tracback time for entropy

variation and DPM method is low include only network delay whereas in PPM tracback time is medium which include network delay plus calculation time.

5.2 AES Encryption Algorithm

AES stands for Advanced Encryption Standard algorithm. It is a bilaterally symmetric Block cipher with a block length of 128,192 and 256 bits which means it uses the same key for both encryption and decryption. But it is found out that the 128 bits block size is the fixed size of block that is being used by many people. It had been used as a symmetric form of encryption.AES algorithm was revealed by bureau in 2001.Dr.Joan Daemen and Dr. Vincent Rijmen 9 are two researchers who developed and submitted Rindael for the AES. The AES algorithms are being used by most of the people at any time so it has become so famous. They are found to be quite helpful to the people and it had also been linked with the data encryption method too. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

An algorithm starts with a random number, in which the key and data encrypted with it are scrambled though four rounds of mathematical processes. The key that is used to encrypt the number must also be used to decrypt it. The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey:

- SubBytes: During this a lookup table is used to determine what each byte is replaced with.
- ShiftRows: In this step, there are a certain number of rows where expect the first row each row of the state is shifted cyclically by a particular offset. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This shifting is applied to all three key lengths.
- The MixColumns: This step is a mixing operation using an inversible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output.
- AddRoundKey: In this last round, derives round keys from Rijndael's key schedule, and adds the round key to each byte of the state. Each round key gets added by combining each byte of the state with the corresponding byte from the round key.

Lastly, these steps are repeated again for a fifth round, but do not include the MixColumns step. Decryption in AES algorithm involves reversing all the steps taken in secret writing improper treatment inverse functions like InvSubBytes, InvShiftRows, and InvMixColumns.

These algorithms basically take basic data and change it into a code known as ciphertext. The larger the key, the greater number of potential patterns that can be created. This makes it extremely difficult to descramble the contents, which is why AES has been Teflon-coated. Eventually, anyone can use AES encryption methods, and it is free for public or private, commercial or non-commercial use.

5.3 J48 Algorithm

J48 is an implementation of C4.5 algorithm, can be used for classification. It builds decision trees from a set of labeled training data using the concept of information entropy. It is classified based on the number of packet sent, packet received, port number and examines the normalized information gain (difference in entropy) that results from choosing an attribute for splitting the data basis on the attribute with the highest normalized information gain is used. Then the algorithm recurs on the smaller subsets. The splitting procedure stops if all instances in a subset belong to the same class. J48 can handle both continuous and discrete attributes, training data with missing attribute values and attributes with differing costs. Following algorithm follows by J48 Decision tree classifier:

- First create a decision tree based on the attribute values of the available training data to classify a new item. So, whenever it meets a set of items (training set) it identifies the attribute that distinguish the various instances most clearly. This feature will help to define most about the data instances so that we can classify them (called highest information gain).
- Now, if there is any value from the possible values of this feature which has no ambiguity means for which the data instances falling within its category have the same value for the target variable.
- Then we terminate that branch and assign to it the target value that we have obtained. For the other cases, we then see for another attribute that gives us the highest information gain.
- Hence we continue in this manner until we either get a clear decision of what combination of attributes gives us a particular target value, or we run out of attributes.
- In the event that we run out of attributes, or if we cannot get an unambiguous result from the available information, we assign this branch a target value that the majority of the items under this branch posses

5.4 KDDCUP'99 Dataset

KDD 99 intrusion detection datasets, which are based on DARPA 98 dataset, provides labeled data for researchers working in the field of intrusion detection and is the only labeled dataset publicly available. It provides benchmark for intrusion detection occurring in the network and also provides designers to evaluate different methodologies [18]. This dataset has about 4, 90,000 single connection records with no redundancy. The KDD Cup 99 data set contains 23 different attack types. Their names are shown in Table II and its features are grouped as follows: Basic Features, Traffic Features and Content Features.

1. Basic features contain all the attributes of the TCP/IP connection and lead to delay in detection. Included features are duration, protocol type, service, flag, src_bytes, dst_bytes, land, and wrong fragment, urgent.

2. Traffic features are evaluated according to the window interval and two features as same host and same service.

(i) Same host feature: It examines the number of connections in the past 2 seconds from the same destination host. The probability of connections will be done in a specific time interval. Included features are dst_host_count,dst_host_srv_count,dst_host_same_srv_rate,dst_host_diff_srv_rate,dst_host_same_src_port_rate,dst_host_srv_diff_host_rate,dst_host_serror_rate,dst_host_srv_serror_rate, dst_host_srv_serror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate.

(ii) Same service feature: It inspects the number of connections in a particular time interval that possesses same service. Included features are count, srv_count, serror_rate, srv_seror_rate,rerror_rate, rv_rerror_rate, same_srv_rate,diff_srv_rate, srv_diff_host_rate.

3. Content features: Dos & probe attack have frequent intrusion sequential patterns compared to R2L & U2R. These two attacks include many connections to several hosts at a particular time period whereas R2L and U2R achieve only a single connection. In order to detect these types of attacks, domain knowledge is important to access the data portion of the TCP packets. Included features are hot, num_failed_logins, logged_in,num_compromised, root_shell,su_attempted, num_root,num_file_creations, num_shells,num_access_files, num_outbound_cmds, is_hot_login, is_guest_login.

Attacks are classified into four categories in KDD CUP datasets where Back, land Neptune, pod, smurf and teardrop comes under the category of Denial of service attack. Satan, ipsweep, nmap and port sweep comes under the category of Probes attack. ftp_write, imap, guess_password, phf, spy and warezclient comes under the category of Remote to local (R2L). Last category of attack is User to root (U2R) includes Buffer_overflow, load module, perl and rootkit.

6. ALGORITHM FOR PROPOSED MODEL

In this section we designed an algorithm for our proposed model. There are two part of this algorithm first part of algorithm define entropy variation where we calculate entropy for legitimate packets and attacks packets. For attack detection used threshold value which is equal to entropy of legitimate user and compare with threshold value. If calculate entropy is less than threshold value then system generate alarm and detect attack. Second part describes the generation of rules from the dataset which classify the attacks such as Neptune, nmap, smurf and Dos attacks.

Algorithm for entropy variation

1. If N->pkt to be send from User to Brk
   Where pkt= No. of packets to be send
2. For each N->pkt
3. Brk will check the pkt which contain text, dataset.
   Where Brk= Broker of the cloud
4. If Ifea will match
   Where Ifea= Stored feature of the Intrusion to classify the type of attack
5. Detect attack for N->pkt and classify type of attack
   End

End

6. for each N->pkt
7. char cx = entry.getKey ()
   double p = (double) entry.getValue() / N
   e += p * log2 (p)
   Where, e is the entropy level of the N->pkt
8. If e<threshold value
   Where threshold value= entropy value of legitimate packets
9. Entropy variates
10. Generate alarm
11. End
12. If N->pkt to be send from Brk-> DC
    Where DC= Datacenter of the cloud
13. End

Generation of Rules from the dataset

1. Rule-1
   If (dst_host_error_rate) >‘0.5’then packet flow is “Neptune”
2. Rule-2
   If (dst_host_error_rate) <=‘0.5’ then
   If (dst_bytes) >‘0’ then packet flow is “Normal”
3. Rule-3
   If (dst_host_error_rate) <=‘0.5’ then
   If (dst_bytes) <= '0' then
   If (src_bytes) <= ‘240’ then Packet contains “nmap” attack
   Else if (src_bytes) > ‘240’ then Packet contains “smurf" attack

Where Attributes shows:

dst_host_error_rate= Rate of connections to the same service coming from different hosts

dst_bytes=number of bytes from destination to source
src_bytes=number of bytes from source to destination

Fig shows the decision tree which is generated on the basis of these generation rules which classify attacks.

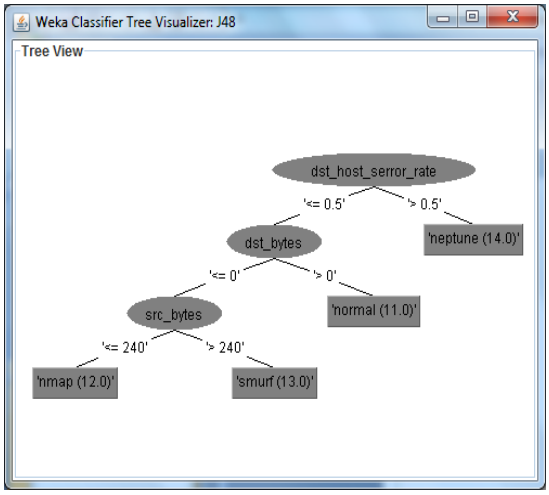

Fig. 2 Attack Classification Decision tree

7. PERFORMANCE EVALUATION

In this section, we present the performance evaluation of proposed IDS system. Performance analysis describes how system can handle more packets and how much time takes to detect attack. Here we are taking different cases and analyzing the performance of system in each case. To evaluate the accuracy of the proposed system we compare it with existing model NICE which is network based approach for multiphase distributed denial of service attacks. Comparison based on success rate which is the percentage of the successfully analyzed packets. The following table shows comparison between Existing Model NICE and Proposed Model

Table 2. Comparison of success rate between NICE and Proposed Model

Traffic Load	Success Rate (%) of NICE	Success Rate (%) of Proposed
<2500	100	99.7
3000	99.89	99.9
4000	99.67	99.9
5000	97	99.9
6000	93	100
7000	94	100
8000	62	100
9000	67	100
10000	68	100
>10000	65	100

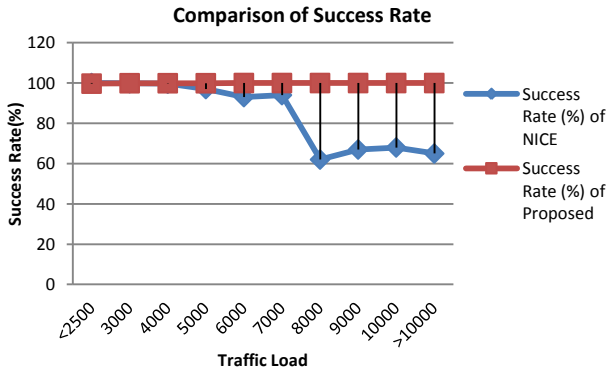

Fig. 3 Graphical view of comparison between NICE and proposed system

Here plotted graph shows Comparison between Existing system a NICE and proposed system and show the proposed system has more accuracy and has much less time to detect attack with respect to traffic load than NICE. Fig.3 shows detection rate which shows number of instances of particular attacks from the total number of instances within datasets.

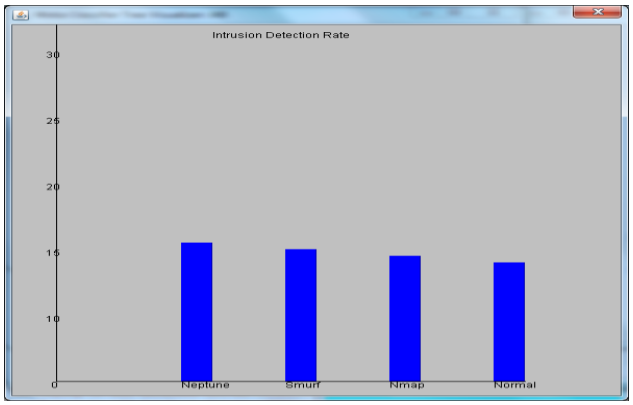

Fig. 4 Detection rate of attacks

Cloud system where thousands of nodes will have big amount of alert raised by IDS. Through this proposed system can also be used to reduce false alarm rate. This approach achieves the design security goals and prevents vulnerable VMs from being compromised in cost effective manner.

To determine performance evaluations, we used four metrics namely CPU utilization which depends on varying traffic load on server, means with increase number of packets per second how much CPU utilize, packet delivery ratio which is the ratio of the number of packets received by the destination to the total number of packet send, processing overhead, network capacity, and communication delay. We performed evaluation through the CloudSim version 3.1 with Pentium 4 or above processor and 100MB or above memory.

8. CONCLUSION AND FUTURE WORK

Cloud Computing provide on demand scalable computing resources to its end users and allows to store their huge amount of data in cloud. These can be exploiting the security risks in cloud. In this paper, we presented intrusion detection system for cloud computing which comprises the concept of entropy variation which is more efficient to traceback attacks compare to other tracback method and J48 algorithm which gives more accuracy to detect attack compare to other decision tree classification algorithm.

The system performance evaluation determines the usefulness of proposed system and shows that proposed solution can significantly reduce the risk in cloud system. The proposed solution can only detect attacks in cloud. To provide better security model prevention system might also be include.

9. ACKNOWLEDGMENT

I would like to give my genuine thanks to my guide Prof. Sreeja Nair who guided me to pursue this topic and helped me to complete this research work.. I believe it my honour to have carried out my research work under her guidance.

10. REFERENCES

[1] M.Malathi, “Cloud Computing Concepts”, 978-1-4244-8679-3/11/$26.00 ©2011 IEEE

[2] Nor Badrul Anuar, Hasimi Sallehudin, Abdullah Gani, Omar Zakari, "Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree", Malaysian Journal of Computer Science, Vol. 21(2), 2008 and On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

[3] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang “NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems”, IEEE Transact

[4] Sandeep K.Sood, "A combined approach to ensure data security incloud computing", Journal of Network and Computer Applications 35 (2012) 1831–1838

[5] Mr. Prashant Rewagad, Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies

[6] Helen Sara George, Mrs.Jeno Lovesum, "A Survey On Different Encryption Schemes And Security Challenges In Cloud Storage System", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013 ISSN: 2278-0181

[7] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 2011

[8] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010)

[9] Nor Badrul Anuar, Hasimi Sallehudin, Abdullah Gani, Omar Zakari, "Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree", Malaysian Journal of Computer Science, Vol. 21(2), 2008

[10] Ahmed Patel, MonaTaghavi, KavehBakhtiyari, JoaquimCelestinoJunior,"An intrusion detection and prevention system in cloudcomputing: A systematicreview", JournalofNetworkandComputerApplications & 2012

[11] Ms Pooja Bhoria, Dr. Kanwal Garg, "Determining feature set of DOS attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[12] Shui Yu, Wanlei Zhou, Robin Doss, Weija Jia, "Traceback of DDoS Attacks Using Entropy Variations", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 3, MARCH 2011

[13] Sharmila Wagh, Anagha Khati, Auzita Irani, Naba Inamdar, Rashmi Soni, "Effective Framework of J48 Algorithm using Semi-Supervised Approach for Intrusion Detection", International Journal of Computer Applications Volume 94 – No 12, May 2014

[14] A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi, "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud", International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013

[15] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009.

[16] Mervat Adib Bamiah, sarfraz Nawaz Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud Computing" International Journal of Advanced Engineering Sciences and Technologies, Vol No. 9, Issue No. 1, pp: 087 – 090

[17] Skoudis E., "Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses". Prentice Hall Inc., 2002

[18] The 1998 intrusion detection off-line evaluation plan. MIT Lincoln Lab., Information Systems Technology Group.http://www.11.mit.edu/IST/ideval/docs/1998/id98-eval-11.tx2, 25 March 1998.