An Alternative Model Of Virtualization Based Intrusion Detection System In Cloud Computing

Partha Ghosh, Ria Ghosh, Ruma Dutta

Abstract: The massive jumps in technology led to the expansion of Cloud Computing as the most accepted medium for communication but it has also increased the scope of attacks as well. So security has become a major issue for Cloud Computing. In this paper we proposed a single IDS Controller creating and managing multiple instances for each user. A multithreaded NIDS protects the cloud efficiently and avoids the traffic congestion for large volume of data. In order to detect encrypted and fragmented data, HIDS is also deployed in the hypervisor for detailed monitoring over Server. Analyzing all the alerts, IDS Controller generates a final report to Cloud Service Provide and an alert report to the cloud user with the help of a Third Party monitoring and advisory service. Our proposed model provides a virtualized environment to protect the Cloud efficiently from vulnerabilities.

Index Terms: Cloud Computing, Cloud Service Provider(CSP), Host based Intrusion Detection System(HIDS), Intrusion Detection System(IDS), IDS Controller, Network based Intrusion Detection System(NIDS), Third Party, Virtualization.

1. INTRODUCTION

Cloud computing is a way to increase capacity or add capabilities of the system on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities [9]. Figure 1 shows a Cloud Computing environment.

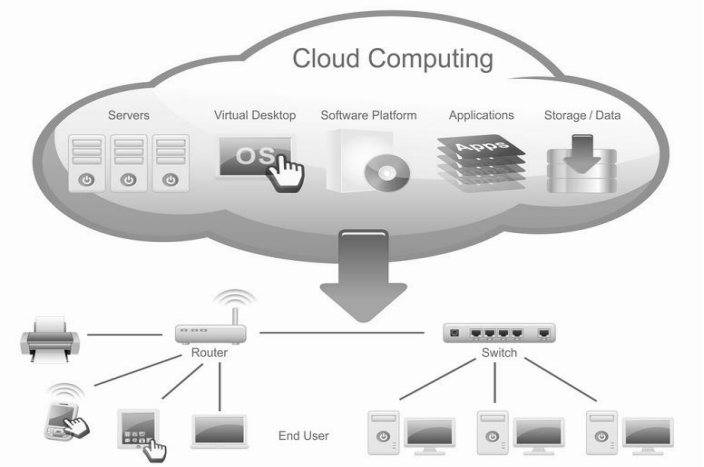

Figure 1. Cloud Computing

- Partha Ghosh, Assistant Professor of Netaji Subhash Engineering College, West Bengal University of Technology, Kolkata, West Bengal, India.
  Email partha1812@gmail.com
- Ria Ghosh, B-Tech student of Netaji Subhash Engineering College, West Bengal University of Technology, Kolkata, West Bengal, India.
  Email ria.mum4@gmail.com
- Dr. Ruma Dutta, Associate Professor of Netaji Subhash Engineering College, West Bengal University of Technology, Kolkata, West Bengal, India.
  Email rumadutta2006@gmail.com

Cloud computing is basically a technology of distributed data processing. It provides scalable information resources and capacities are provided as a service to multiple external customers through Internet technology. There are various service models developed, broadly divided into three layers: Infrastructure-as-a-Service (IaaS)—the Infrastructure services layer, Platform-as-a-Service (PaaS)—the Platform layer, Software-as-a-Service (SaaS)—the Application layer [6]. In the case of IaaS servers, network devices, and storage disks are made available to organizations as services on a need basis. PaaS provides a platform for creating applications which are developed completely from the Internet. PaaS does not require downloading or installing software. SaaS includes applications that run off the Cloud and are available to Web users or enterprises on a pay-as-you-go, anytime-anywhere basis [5]. Cloud services can reduce the cost and overhead of owning and operating computers and network. In spite of many advantages of cloud as it is distributed system, it can be attacked by distributed intrusion attacks as Denial of Service (DOS) or Distributed Denial of Service (DDOS), Cross Site Scripting (XSS) etc. [3]. DDOS or DOS attack is an explicit attempt by attackers to prevent legitimate users of a service from using that service. A DDOS attacker uses many machines to launch a coordinated DOS attack against one or more targets [12]. XSS attacks are code injecting attack by which an intruder can inject malicious content into web page [14]. So to protect the cloud users and the data from these vulnerabilities, a strong defensive system is necessary. For this security purpose, firewall alone may not be efficient. Firewall has holes to access the Internet or send or receive email. If any intrusion gets through these holes it can harm the system or network [13]. So an Intrusion Detection System (IDS) is required to find the attacks in cloud. There are broadly two types of Intrusion Detection Systems, they are Host based intrusion detection system (HIDS) and Network based intrusion detection system (NIDS). HIDS works on a particular host machine and allow only the administrator aware of it [7]. HIDS requires software or agent components running on a particular host. NIDS monitors the entire network or a segment of a network system instead of focusing on a particular host machine only. It actually works for all the hosts connected in that network system by analyzing the network packets [7]. There are several advantages and disadvantages of HIDS and NIDS. Considering the overall feature of HIDS and NIDS, an Intrusion detection system is being chosen for

any system on network. As HIDS works on a particular host it can give detailed information about system activity more accurately than a NIDS can give and generates less false positive alarms. Host based sensors are useful to detect attacks in a particular host machines and protect those from internal and external attacks. HIDS also can work over encrypted and fragmented data but NIDS cannot [10]. NIDS placed on strategic point(s) in network system and monitors inbound and outbound network traffic [8]. Although having these advantages HIDS cannot detect attacks on network traffic since they are made to run on a single system. So for any enormous network traffic and data flow HIDS is not at all an intelligent choice. Also it will be economically high. In this case NIDS is a good match. Also NIDS does real time detection. Traditional NIDS will not be able to handle the data packets if the volume of network traffic is very high. It may lead to network congestion and packet loss. In this scenario a multithreaded NIDS can be a good alternative [3]. Multithreaded NIDS contains shared queue in which every process can have multiple threads which work in a collaborative fashion to improve the system performance and handle large amount of data. However, the system that involves both the host-based and network-based systems are more acceptable approach for cloud computing environment because they offer significantly different benefits. A HIDS monitors the system activities of hypervisor continuously and detect system intrusion. NIDS works on the network packets, detects the network anomalies. Cloud processes a large number of requests as per as user demand. So if HIDS is deployed it will lead to performance loss which will decrease the rate of flow of packets. In this case NIDS is a intelligent alternative as it does not use system resources to analyze data packets. It also nullifies the requirement of loading software in different host machine at network. As in cloud network, the volume of traffic is high, traditional NIDS will lead to network congestions and may be overloaded. It is noted that if single IDS is implemented for an entire network in Cloud, the load on it increases as the number of host increase. Apart from that it is difficult to control different kinds of attacks acting on each of the host present in the network [2]. So to effectively protect the Cloud users IDS should have the ability to expand. For this the use of virtualization in Intrusion Detection System is done in our paper. Virtualization can help any organization of system to obtain certain gain in efficiency and cost effectiveness. This technique also increases scalability and improves time complexity. Virtualization basically allows one computer to do the job of multiple computers, by sharing the resources of a single hardware across multiple environments. Virtualization allows multiple operating system instances to run concurrently on a single computer. Cloud is difficult and inefficient without virtualization [4]. A virtualized IDS is proposed in this paper along with a multithreaded IDS to maintain the huge network traffic and to protect the cloud in every possible way from vulnerabilities.

2. LITERATURE REVIEW

2.1 Analysis

Cloud computing is a technique to provide services to users using Internet. With the rapid increase of resources in cloud, attacks are becoming more prevalent. To secure the cloud from intrusion, firewall is not sufficient. An Intrusion Detection System (IDS) is needed for protecting the cloud environment in a better way. Intrusion Detection is a technique used to monitor and detect suspicious activity both at the network and host level. Intrusion Detection System (IDS) monitors the events happening on a host or in an entire network system, analyses them and alerts the administrator in case of any suspicious or malicious activity detected. In some cases IDS takes some action against abnormal activities by blocking malicious network packets or user [8]. The ultimate goal of IDS is to identify all attacks and make the system secure from vulnerabilities. As Cloud is distributed it can be attacked easily, so IDS becomes crucial for cloud environment. IDS uses two detection methods to detect attacks. Knowledge Analysis and Behavioral Analysis. Knowledge based IDS catches the intrusions in terms of the characteristics of known attacks or system vulnerabilities. This type of detection uses a predefined rule set and features are extracted from known intrusion. The rule sets reside in a knowledge base and we can update the knowledge based by adding new rule without modifying existing ones. This method is very accurate and generates much fewer false alarm. But it can not detect novel or unknown attack. Behavioral Analysis is based on audit data collected over a period of normal operation. In this method any action that significantly deviates from normal behavior is considered as intrusion [11]. This method is limited by training data, so it may generate high false alarm. But the method can detect unknown attacks and able to cover a wider range of attacks.

2.2 Related works

To efficiently protect the Cloud an Intrusion Detection System requires virtualization-based approach. Cloud services allow users to use software and hardware that are managed by cloud service provider on pay as you use basis at remote locations. Confidentiality of cloud data, cloud security auditing, network and host based attack on the remote server and lack of data interoperability are some major security issues in Cloud Computing. A number of Intrusion Detection Systems have been studied. In paper [1], Vieira et al. proposed a HIDS-based architecture for cloud computing. In this model IDS has two components Analyzer and Alert System. Here IDS service gets all the captured data by event auditor. IDS service detects all the known and unknown attacks using behavior-based or knowledge-based approach. When an attack is detected, alert system inform other nodes. This model can generate a very low rate of false positive and false negative alarm rate for behavior analysis. But this model can't detect any insider intrusion which is running on VMs. In paper [2], Dhage et al. proposed a Virtualized Intrusion Detection System for Cloud Computing. In this model different instances of IDS for each user are created and monitored by single controller. Whenever any user starts to access any cloud service an instance of IDS for that particular user is created in order to monitor and achieve protection. These instances are called as 'Mini IDS'. These instances are deployed between each user and Cloud Service Provider. Each instance monitors the activity of that particular host machine it is created for and at the end of a session it sends a log of that session to IDS Controller. This information is stored in cloud logs and retrieved again from knowledge base by IDS controller when the user starts the next session. The knowledge base, stored in the cloud, contains information about the patterns of user activity based on information in the log of the cloud. Every time, an instance of IDS is provided for a particular user, information about their

previous activities are required by IDS Controller from the knowledge base. To detect any intrusion from user this pattern of activity can be observed, it is possible to apply different rules to different users. In this architecture every user and IDS instance assigned a one to one relationship between them, but there is a many to many relationship between the IDS instance and node controller. IDS controller works through three terms such as Agents, Directors and Notifies. Agents capture the information from data sources of log files, processes, and network and send them to the Directors. The Agents are located within the IDS instances. The Directors, located in the IDS controller, make the analysis of the information, which determines whether an attack is happening or not. In case of a possible attack, Notifier takes the necessary actions. Here one single IDS Controller is deployed for a Cloud Service Provider. It creates and manages instances of IDS for each user. These instances monitor user activities. From this paper we have got an idea of virtualization using IDS Controller. An effective Intrusion Detection System is required to handle the broad network access and rapid elasticity of Cloud. To deal with the enormous network traffic of cloud, a multithreaded cloud NIDS is introduced in paper [3]. Multithreaded NIDS is capable to process multiple packets at the same time and reduces the rate of packet loss and risk of overloading the NIDS causing congestion. Simultaneous processing of process, increase the overall performance of Cloud. Multithreaded NIDS works through three modules in cloud. Those are capture & queuing module, analysis/processing module and reporting module. Capture module catches the data packets (ICMP, TCP, IP, and UDP) from network traffic. The captured data packets are sending to the shared queue for analysis. Shared queue sends those data packets to analysis and process module where they are analyzed against a signature base and a predefined rule set. Each process in shared queue can have multiple threads to increase the cloud performance. This model also includes a third party monitoring and advisory service that receives alarm from NIDS. The third party analyzes the alarm and generates a report for cloud user information as well as sends a comprehensive expert advisory report to Cloud Service Provider. Here users can get to know about the harmful attacks and have an idea about how much secure their data is under that cloud server side. From this paper we have got the idea of an efficient multithreaded cloud NIDS and a third party monitoring and advisory service.

3. PROPOSED WORK

Cloud computing is an internet based computing of resources where instead of storing data in user own hard drive or updating applications, they use a service over internet based on the concept of virtualization of resources as a service on pay-as you-use basis. It is very important to provide the best security for cloud computing environment and for this it is necessary to have Intrusion Detection System (IDS) available anywhere in Cloud. Many approaches on Intrusion Detection System have been proposed till now. In this paper a Virtualized Intrusion Detection System is proposed to handle the large scale network access traffic and protect the data and applications in cloud from malicious attack and vulnerabilities. Cloud model is inclined to attackers for its elasticity and major availability of resources. To protect the cloud effectively an IDS should have the ability of expand and increase or decrease the number of sensor as per as user demand. Here in this paper we introduce a cloud intrusion detection system having the characteristics of virtualization to provide a better security in cloud environment. This model also includes multithreaded cloud NIDS and third party monitoring and advisory service technique. This proposed model provides both the advantages of Virtualization of IDS and Multithreaded cloud IDS. Virtualization of IDS is done by an IDS Controller and the multithreaded cloud IDS (basically NIDS is used here) manages the heavy flow of network traffic. The components of our proposed model are basically IDS Controller, Multithreaded Cloud IDS, Third party monitoring and advisory service, Cloud Servers (HIDS based hypervisor). An IDS controller will create different instances of IDS for each user and these instances are deployed between each user and Cloud Service Provider (CSP). These instances are named as “Mini IDS” and it will work on each specific user. Multithreaded Cloud IDS is deployed on the bottleneck of network points such as router, gateway outside the virtual machine and monitor the network traffic. The third party monitoring service is for monitoring the alerts sent by cloud IDS and generating advisory reports to IDS controller. The IDS Controller reduces the workload of single IDS for cloud environment. It also generates a final advisory report to CSP and a alert report to cloud users. Figure 2 shows the architecture of our proposed model.

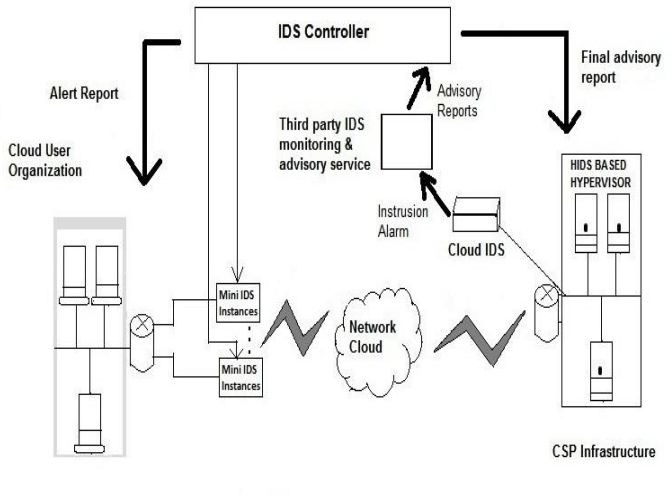

Figure 2. Proposed Cloud IDS Model

This proposed model is based on the concept of ‘Virtualization of IDS’ in cloud environment. Whenever a user starts a session an instance of IDS i.e. Mini IDS is created and works on the specific user. It monitors, supervises and achieves protection. Mini IDS contains a term called Agent. Each instance supervises on each user activities and sends a report of all the activities to the IDS Controller via cloud NIDS after the end of each session. IDS Controller manages all the instances. IDS Controller works through three steps named as Agents, Directors and Notifiers. Information from the data sources of log files, processes and network are captured by agents and are sent them to director. Agents lie in IDS instances and Directors are located in the IDS Controller. Directors make the analysis of information, which determines whether an attack is happening. Notifier takes the necessary action. To handle the heavy flow of network traffic a

multithreaded cloud IDS is placed on the bottleneck of network points such as router, gateway outside the virtual machine and monitor the network traffic. The cloud user accesses its data on remote servers at service provider's site over the cloud network. The requests sent by the users to Cloud Service Provider (CSP) and user activities are monitored and logged through the multithreaded NIDS. This multithreaded NIDS work through three modules: capture & queuing module, analysis or processing module and reporting module. The data packets are captured and sent to the shared queue for analysis by captured module where the data packets are analyzed against network based anomaly detection. To increase the performance every processes of this shared queue uses multiple thread and thus system performance goes high. After an efficient analysis an alert is generated. Reporting modules read those alert and make a report according to them. NIDS can handle the network anomalies but it cannot work on encrypted and fragmented packets. A HIDS is deployed in the hypervisor in order to work on encrypted and fragmented data on the basis of signature and behavioral analysis on them. Agents present inside IDS instances capture information from the data sources of log files, processes, network and send them to the multithreaded cloud NIDS via network cloud. This user's information and report produced by reporting module of NIDS are sent to a third party monitoring service. Third party monitoring and advisory service having experience and resources, analyzes them and sends an advisory report to IDS Controller. The IDS controller finally generates the final report, analyzing this advisory report sent by third party and the report issued by notifier on the basis of information from Mini IDS i.e. IDS instances. The IDS Controller monitors the user activity on the basis of analysis, sends a final report to CSP and an alert to cloud user. This Model includes both the knowledge based detection method and behavioral based detection method. IDS Controller uses knowledge based (also known as misuse based) to detect intrusion. The information about user activities sent by IDS instances to IDS Controller are stored in the cloud by IDS Controller as a knowledge base. This knowledge base contains the information of the pattern of user activities and this is stored in the Cloud. Every time a user starts a new session the previous activities of the user are retrieved by the IDS Controller and this pattern or profile is needed to detect any intrusion. Cloud NIDS use behavioral or anomaly based intrusion detection as well as knowledge based intrusion detection to find out the vulnerabilities in the data in network. The data packets are captured and sent to the shared queue for analysis by captured module where the data packets are analyzed against a predefined rule set. NIDS catches the ICMP, TCP, IP, UDP packets from network traffic and analyzes them using network based anomaly detection. NIDS tackles a huge amount of data and it is very efficient, but it fails to work on fragmented and encrypted data packets. This drawback can be demolished by the HIDS deployed in hypervisor. It works on the server and analyses the encrypted and fragmented data by signature and behavioral analysis on them. HIDS does not have to do any network level detection. Third party analyzing and monitoring service analyzes the alerts sent by NIDS and sends them to IDS Controller. Figure 3 shows the flowchart of our proposed model. The main advantage of our proposed model is reduction the workload from a single IDS for Cloud. Whenever users want to access the Cloud this one is split between multiple instances of the IDS to carry out their work in a better way than with single IDS for the whole Cloud. As per user's requirement the number of sensors or instances of IDS can be rapidly increased and decreased. Users activities are monitored by Mini IDS's. HIDS monitors over hypervisor. So workload from multithreaded cloud NIDS is got reduced by Mini IDS's and HIDS. Multithreaded Cloud NIDS monitors the inbound and outbound data packets. Mini IDS's will monitor each of the user activity and multithreaded cloud NIDS will monitor the inbound and outbound data packets. Implementation of NIDS can reduces the CPU, memory consumption as well as packet loss and helps to improve the overall performance of Cloud IDS. Host based IDS can work only on host machine. So if attackers become able to attack the host machine i.e. hypervisor they would not allow HIDS to send alerts to administrator. A NIDS monitors the entire network traffic and checks all the packets header for malicious attacks. Multithreaded NIDS handles a large amount of data and works very efficiently. This dedication of NIDS makes the job of HIDS easier. HIDS need not do any networks level analysis. It works only on the hypervisor and analyzes the encrypted and fragmented data. Using of IDS Controller, Multithreaded NIDS, HIDS based hypervisor together reduce the workload from each other as well as give a better security against malicious attacks. Information from the data sources of log files, processes and network captured by agents are sent to the Cloud NIDS via network cloud and the user activities are monitored twice, firstly by IDS instances and later by Cloud NIDS. The intrusion alarm generated by reporting module in NIDS is sent to the third party monitoring and advisory service. This third party analyses them and sent an advisory report to IDS Controller. The IDS controller finally generates and sends the final report to Cloud Service Provider and an alert report to Cloud users.

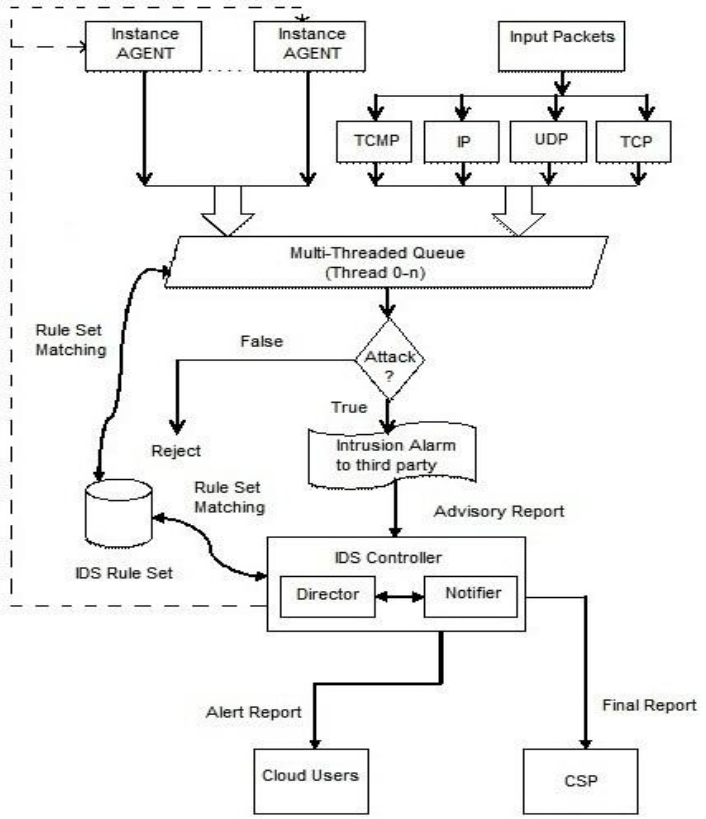

Figure 3. Flowchart of our proposed model

4. CONCLUSION

Security in cloud has become an important issue as data are transferred and exposed through the network. It is very much essential to keep out intruders from network where high rate of data traffic is accessed. It is also required to increase performance of the system and decrease the cost. The virtualization serves this purpose. But virtualization is prone to attacker for its distributed environment. So to protect the cloud efficiently the best solution is that incorporate both NIDS and HIDS. An efficient, reliable and scalable Intrusion Detection System is needed for Cloud environment. Our proposed solution uses a Virtualized IDS system and both NIDS and HIDS efficiently to block malicious traffic. It generates a report with the help of both IDS Controller and Third Party monitoring and advisory service to Cloud Service Provider and also generates an alert report for Cloud users.

REFERENCES

[1] Vieira K, Schulter A, Westphall C, Westphall C. Intrusion detection techniques in grid and cloud computing environment. IEEE IT Professional Magazine, pp.38-43 (2010).

[2] Dhage S N, Meshram B B, Rawat R, Padawe S, Paingaokar M, Misra A. Intrusion Detection System in Cloud Computing Environment. International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, pp.235-239(2011).

[3] Shelke P K, Sontakke S, Gawande A D. Intrusion Detection System for Cloud Computing. International Journal of Scientific & Technology Research Vol.1, Issue 4, pp.67-71(2012).

[4] Araújo J D, Abdelouahab Z. Virtualization in Intrusion Detection Systems: A Study on Different Approaches for Cloud Computing Environments. IJCSNS International Journal of Computer Science and Network Security Vol.12, pp.9-16(2012).

[5] Mohod A G, Alaspurkar S J. Analysis of IDS for Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM) Vol.2, Issue 3, pp.344-349(2013).

[6] Ubhale P R, Sahu A M. Securing Cloud Computing Environment by means of Intrusion Detection and Prevention System (IDPS). International Journal of Computer Science and Management Research Vol.2, Issue 5, pp.2430-2435(2013).

[7] Zarrabi A, Zarrabi A. Internet Intrusion Detection System Service in a Cloud. IJCSI International Journal of Computer Science Issues Vol.9, Issue 5, pp.308-315(2012).

[8] Agrawal G, Kamble M, Proposed Multi-Layers Intrusion Detection System (MLIDS) Model. International Journal of Computer Science and Information Technologies (IJCSIT) Vol.3, pp.5040–5042(2012).

[9] Charan N R G, Rao S T, Srinivas P V S. Deploying an Application on the Cloud. (IJACSA) International Journal of Advanced Computer Science and Applications Vol.2, pp.119-125(2011).

[10] Gupta P, Kaliyar P. History Aware Anomaly Based IDS for Cloud IaaS. International Journal of Computers & Technology Vol.10, pp.1779-1784(2013).

[11] Singh S K, Chaurasia N, Sharma P. Concept & Proposed Architecture of Hybrid Intrusion Detection System using Data Mining. International Journal of Engineering and Advanced Technology (IJEAT) Vol.2, Issue 5, pp.274-276(2013)

[12] Gupta B B, Joshi R C, Misra M. Distributed Denial of Service Prevention Techniques. International Journal of Computer and Electrical Engineering Vol.2, pp.268-276(2010).

[13] Kanika, Urmila. Security of Network Using Ids and Firewall. International Journal of Scientific and Research Publications Vol. 3, Issue 6, pp.1-4(2013).

[14] S Shalini, S Usha. Prevention Of Cross-Site Scripting Attacks (XSS) On Web Applications In The Client Side. International Journal of Computer Science Issues (IJCSI) Vol.8, Issue 4, pp.650-654(2011).