State of the Art Study of Intrusion Detection System for Cloud Computing

Mohammed Yesuf Getu[1], Husain Shahnawaz[1]
[1]Department Computer Science, College of Engineering and Technology, Samara University, Samara (Ethiopia)
Email:mmm.y2007@gmail.com, shahnawaz.husain@gmail.com

ABSTRACT Industrialization of Cloud Computing platform opens the doors for the technology but as well it raises the security concerns for the stakeholders of the technology. Cloud computing is a "network of network" over the internet and possible backbone of development and deployment of services, therefore possibilities of intrusion is more with the intensification of erudition of intruder's attacks. For cloud computing, enormous network access rate, relinquishing the control of data and application to service providers and distributed attacks vulnerability, an efficient, reliable and information transparent a very powerful security system not only the intrusion prevention system but also an Intrusion Detection System is obligatory. In this paper, a state of the art study for cloud computing features and IDS models as well as the key players of the technology and open source simulators to support the researchers and for a better and optimized efficiency and transparency for the cloud services.

Keywords: Cloud Computing, Intrusion detection system, SaaS, PasS, IaaS, security, simulator.

1. INTRODUCTION

Peoples has reliant on technology, over the last decade. Tremendous growth on the market of stock prices, receive news, email and ecommerce business shows that peoples are depend on the networks and technology. The integrity and availability of all these systems need to be defended against a number of threats. Hackers, rival **firms**, terrorists and even foreign governments have the motive and capability **to hold** out **subtle** attacks against systems [1]. Therefore, the information security field will play a vital role to the safety and economic fortune of the society as a whole. The mounting advancement and prevalent use of electronic data processing and electronic business conducted through the massive use of the wired and wireless communication networks, Internet, Web application, cloud computing along-side varied occurrences of act of terrorism, raises the necessity for providing secure and safe information security systems through the use of firewalls, intrusion detection and prevention systems, encryption, authentication and other hardware and software solutions. Cloud Computing technology offers ubiquitous, opportune, demand-based access to a shared group of configurable computing resources (like storage, network, services applications and servers) that can be quickly provisioned and released with least management effort or service provider interactions [3].

Cloud computing can be defined as an internet-based computing where by shared resources, software and information are provided to the users on the basis of their demand. Cloud computing has been evolved and rapidly developed together with the trend of IT services. A cloud computing service is a novel model of computing in which people need to pay only for the use of services without cost of purchasing the software's and infrastructures. In contemporary, information system security has become a growing concern for the systems globally. Systems become gradually vulnerable due to the rapid increase in inter-connectivity and accessibility, which has resulted in more frequent intrusions, misuses and attacks. Intrusion detection attempts to detect computer attacks by inspecting data records observed by processes on the same network [6]. Cloud computing provides a framework for supporting end users easily attaching powerful services and applications through internet. Denial-of-services (DoS) attack or Distributed Denial-of-Services are the major security concern in cloud based environment. To protect the cloud environment from these attacks best solution is to use Intrusion Detection System's (IDS) [7]. Due to distributed environment, cloud computing is the most vulnerable targets for intruder's attacks. IDS is an artificial intelligent agent which enhance the security measures by the use of systematic data logs examination, configurations, network traffics and other peripherals. Traditional IDSs are not suitable for cloud environment as network based IDSs (NIDS) cannot detect encrypted node communication, also host based IDSs (HIDS) are not able to find the hidden attack trail. Kleber, schulter et al. [11] have proposed an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behavior-based (comparison of recent user actions to usual behavior) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion. The authors have tested their IDS prototype with the help of

simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies compliance check for cloud service provider and their reporting procedures to cloud users.

Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization. IDS implementation in cloud computing requires an efficient, scalable and virtualization-based approach. In cloud computing, user data and application is hosted on cloud service provider's remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Although the administrator of cloud IDS

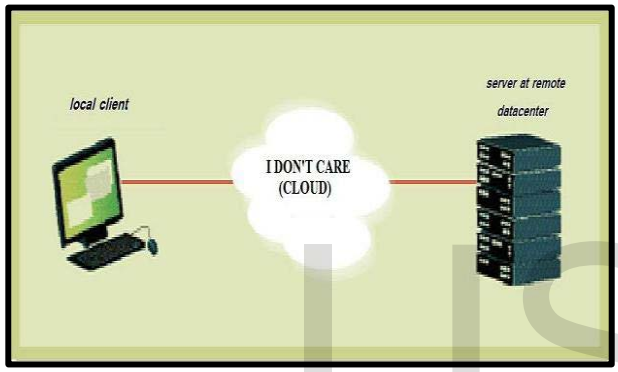

Figure 1: The Cloud Is Not Bothered About The Outer Environment [30]

should be the user and not the provider of cloud services. Roschke and Cheng et al. [2], have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format (IDMEF) standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to 'Event Gatherer' program. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyzes complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user. Cloud computing describes a data-processing infrastructure in which the application software, and often the data itself stored permanently not on your PC but rather a remote server that's connected to the Internet. When you need to use the application or access the data, your computer connects to the server through the Internet and some of that information is cached temporarily on your client machine. The cloud revolves around one single concept. **"I DON'T CARE"** as shown in Figure1. As the name suggests, the function of the cloud is to provide individuals and small and mid-sized businesses access to an array of powerful applications and services through the internet and not concerned about the basic underlying complexities involved in delivering services. Cloud is accessible through any digital device—be a laptop, a cell phone or a smart phone that are capable to connect to internet, cloud based services like web-mail, social networking, photo sharing, and video viewing are already interwoven into fabric of our daily lives.

While the very definition of Cloud suggests the decoupling of resources from the physical affinity to and location of the infrastructure that delivers them, many descriptions of Cloud go to one extreme or another by either exaggerating or artificially limiting the many attributes of Cloud. This is often purposely done in an attempt to inflate or marginalize its scope. While the very definition of Cloud suggests the decoupling of resources from the physical affinity to and location of the infrastructure that delivers them, many descriptions of Cloud go to one extreme or another by either exaggerating or artificially limiting the many attributes of Cloud. This is often purposely done in an attempt to inflate or marginalize its scope. The Characteristics of cloud computing is described as [32]:

a. **Virtual** – Physical location and underlying infrastructure details are transparent to users.
b. **Scalable** – Able to break complex workloads into pieces to be served across an incrementally expandable infrastructure.
c. **Efficient** – Services Oriented Architecture for dynamic provisioning of shared compute resources.
d. **Flexible** – Can serve a variety of workload types – both consumer and commercial.

As cloud computing has taken hold, there are six major benefits that have become clear [32]:

a. **Anywhere/anytime access** It promises universal access to high-powered computing and storage resources for anyone with a network access device.
b. **Specialization and customization of applications** it is a platform of enormous potential for building software to address a diversity of tasks and challenges.
c. **Collaboration among users** cloud represents an environment in which users can develop software-based services and from which they can deliver them.
d. **Processing power on demand** – the cloud is always on computing resource that enables users to tailor consumption to their specific needs.

e. **Storage as a universal service** – the cloud represents a remote but scalable storage resource for users anywhere and everywhere

f. **Cost benefits** – the cloud promises to deliver computing power and services at a lower cost. The major portion of industry cost about 50 % goes to obtain the strategic project raw materials. If these are available on cloud, the 50% cost employed is eradicated as shown in figure 2.

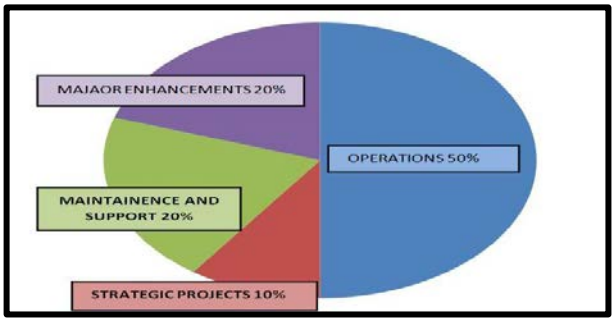

Figure 2: Operations Compute 50% of Cost of Projects Can be Eradicated with Cloud [30]

Looking at the list of benefits, they actually highlight what we think are the top three concerns organizations have with Cloud computing. It revolves around understanding how:

a. **S**oftware A**s a S**ervice **(SaaS**) provides a large amount of integrated features built directly into the offering with the least amount of extensibility and a relatively high level of security. Since the user can only access or modify the data on the pre-defined application the underlying security issues are not of much concern.

b. **P**latform As **A S**ervice **(PaaS**) generally offers less integrated features since it is designed to enable developers to build their own applications on top of the platform and is therefore more extensible than SaaS by nature, but due to this balance trades off on security features since user is responsible for program security and security issues.

c. **I**nfrastructure **A**s **A S**ervice **(IaaS)** provides few, if any, application-like features, provides for enormous extensibility but generally less security capabilities and functionality beyond protecting the infrastructure itself since it expects operating systems, applications and content to be managed and secured by the consumer.

In the Cloud computing environment, the deployment of already available Intrusion Detection and Prevention Systems (ID/PS) can't achieve the desired level of security and performance since architecture of cloud computing paradigm is different from existing computing methods like Grid computing. The rapidly growing demand of cloud resources by its users urges the need of some efficient mechanism for secure provisioning of its resources since intruders may compromise the cloud resources and can cause damages to users' data stored there. A. Patel et al. [15] has emphasized the need to develop an IDPS that is specifically designed according to the characteristics of cloud rather than deployment of a traditional IDPS. For this, authors recommended the use of four novel concepts namely; autonomic computing, fuzzy theory, ontology, and risk management. Autonomic computing is the on demand, self-management capability of cloud resources. Fuzzy logic works on the basis of degrees between false and truth, or 0 and 1. It is a probabilistic approach to reach a conclusion instead of using exact values. Risk manager works in assistance with Fuzzy logic to analyze system vulnerabilities, manage false positive rate, and help in calculation of risk severity level for taking appropriate action. Ontology refers to the representation of knowledge in the form of a set of concepts.

The effectiveness of IDS depends on aspects like the detection method, location of IDS in network, and its configuration [12]. In cloud, the IDS can be installed at different locations like: at the boundary of a network, at a host, at a VM/hypervisor, or distributed across all regions of cloud. The detection method used by IDS may be signature based, anomaly based, or hybrid. The incorporation of soft computing techniques like Fuzzy Logic, Artificial Neural Networks (ANN), Support Vector Machines (SVM), association rules and Genetic Algorithms (GA) or a hybrid combination of any of these to increase the performance of signature based or anomaly based IDS [8]. An IDS is a software that automates the intrusion detection process and detects possible intrusions. An IDPS is a software or hardware device that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. IPSs are differentiated from IDSs by one characteristic; IPS can respond to a detected threat by attempting to prevent it from succeeding [13]. The IPS changes the attack's content and/or changes the security environment. It could change the configuration of other security controls to disrupt an attack, such as reconfiguring a network device to block access from the attacker or to the victim, or altering a host-based firewall on a target to block incoming attacks. Some IPSs can remove or replace malicious portions of an attack to make it benign. Because of the high false alarm rates of the anomaly detection [14], IPS incorrectly identifies a legitimate non-intrusive normal activity as malicious and responds to that detected activity inaccurately.

The rest of the paper is divided in the sections, section two describes the security concerns related to cloud computing deployment, section three deals with the literature review of IDS system for cloud environment, section four describes the classification of IDS systems with respect to cloud computing, section five explains the available best simulators for cloud

computing, section six emphasis on the importance and future of cloud computing in context of industrialization.

2. SECURITY ISSUES IN CLOUD COMPUTING

Security has always been the main issue for IT Executives when it comes to cloud adoption. However, cloud computing is an agglomeration of technologies, operating system, storage, networking, virtualization, each fraught with inherent security issues, resembling browser based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing[4]. Security threats can be categorized as follow:-

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

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

2.3 Lack of Data Interoperability Standards: It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user's data and application may not be compatible with other vendor's data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider [5].

2.4 Network and Host Based Attacks on Remote Server: Host and network intrusion attacks on remote servers are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users.

2.5 Sub-Contracting Cloud Services: Cloud user makes a contract or agreement for service provisioning with the cloud service provider. Subcontracting of cloud services by cloud service provider to another service provider poses security issues like non-repudiation or not owing the responsibility, if some-thing goes wrong with precious data and application of cloud users.

2.6 Non-Availability of Cloud Services: Non-availability of services due to Cloud outages can cause monetary loss to cloud user organization. A deliberate and comprehensive Service Level Agreement (SLA) must be written among user and provider covering all the relevant legal and service provisioning issues and details.

3. LITERATURE REVIEW

Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infrastructure, to each consumer. Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server Based Computing(SBC), and Network Computing, rather than entirely new type of computing technique[3][4]. Parag K. Shelke [5] concludes that providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. Distributed model of cloud makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of service (DDOS) and Cross Site Scripting. To handle large scale network access traffic and administrative control of data and application in cloud, a new multithreaded distributed cloud IDS model has been proposed. Our proposed cloud IDS handles large flow of data packet, analyze them and generate reports efficiently by integrating knowledge and behavior analysis to detect Intrusion. Mohammad sazzadul hoque [10] describes, nowadays it is very important to maintain a high level security to ensure safe and trusted communication of information between various organizations. But secured data communication over internet and any other network is always under threat of intrusions and misuses. So Intrusion Detection Systems have become a needful component in terms of computer and network security. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely. In this progression, here we present an Intrusion Detection System (IDS), by applying genetic algorithm (GA) to efficiently detect various types of network intrusions. Parameters and evolution processes for GA are discussed in details and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity. S. N. Pawar [7] Describes the intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks since the increased connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification. Intrusion detection systems are used to detect unauthorized access to a computer system. A number of soft computing based approaches are being used for detecting network intrusion. This paper presents a survey on intrusion detection

techniques that use genetic algorithm approach. Monjur Ahmed [9] Describe security issues in the cloud computing. Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud architecture. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility, and advantages that cloud computing has to offer will have little credibility. This paper present a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing.

4. CLASSIFICATION OF IDS FOR CLOUD ENVIRONMENT

In this section, we will describe various CIDS and classify them into three types based on the intrusion detection technique used by each system. The types are **Signature based, Anomaly based and Hybrid**. We have investigated systems from each category and analyzed them to evaluate whether or not they meet the security requirements of cloud.

4.1 Signature Based IDS: C. C. Lo et al. has proposed and simulated an IDS that works in cooperative way to counter the DoS and DDoS attacks [16]. It consists of four components each with a specific role. The first one performs intrusion detection by capturing and analyzing the network packets. It instantly drops the packets exhibiting a correlation with the block table rules, or else the abnormal packets having no correspondence to these rules are forwarded to the alert clustering component which identifies the alert level of received suspicious packet. The third component blocks intrusion packets and sends alerts to other IDSs. The fourth component collects alerts from other IDSs and performs majority vote to make decision about packet. We can protect the system from single point of failure attack by deploying the proposed IDS. However, it cannot detect unknown attacks since it uses signature based detection techniques to detect intrusions. C. Mazzariello et al. has tested the deployment of IDS at various positions in cloud to detect DoS attacks on virtual SIP-based hosts [18]. The authors have utilized Eucalyptus as the cloud and snort as network based IDS to perform the experiments. Two of the six physical machines are hosting eight virtual machines. Two security groups are created, each containing one SIP server, one Apache web server and many RTP –based agents. To generate background traffic, D-ITG is used. "Inviteflood" tool is used to generate the SIP flood traffic. The authors have considered two scenarios to evaluate the IDS performance based on its position in the cloud. Evaluation results have shown that detection of DoS attacks using single IDS instance placed close to the Cloud Controller (CC) will significantly increase the load on CC. Conversely, deployment of separate instance of IDS at each virtual machine affects only the CPU load of attacked VM and there is no significant impact on other VMs. The proposed technique is signature based so unable to detect unknown attacks. A. Bakshi et al. has proposed and implemented a solution for detection of DDoS attacks [19]. The idea is to install IDS (e.g. snort) on a virtual switch which logs the incoming/outgoing traffic to be audited into a database. The IDS performs real-time detection of specific attacks (based on
rules) by analyzing the network packets. If IDS observes a large number of packets from specific IP addresses (DDoS attack), it
reports to virtual server which blocks IP addresses of all zombies that form the botnet. Moreover, the virtual server shifts the applications under attack to VMs hosted in a separate datacenter and routing tables are updated.

4.2 Anomaly Based IDS: A. Patel et al. has proposed an autonomic agent-based intrusion prevention system using the principles of autonomic computing [20]. The detection methodology is anomaly based. Autonomous sensors are used to monitor the network traffic and system activities (e.g. system calls, file access and modifications) for identification of suspicious activity. In this paper, our method increases resource availability of Cloud Computing system and handle the potential threats by deploying Multi-level IDS a managing user logs per group according to anomaly level. We can suppose that VMs have equal quantity of resource, then host OS can assign less guest OS with IDS, because IDS use much resource. On the other hands, we can assign more guest OS with Multi-level IDS, because medium level and low-level IDS use less resource. The users classified as high-level group are potentially dangerous user, therefore a high-level IDS consumes much resource to detect all of anomalous behaviours. However, a low level IDS consumes less resource, because the user classified as low-level group are judged that they are normal user. As a result, low-level IDSs maintain little rules for managing effective resource, so it can assign more guest OS than high and medium-level. Our method also supports classifying the logs by anomaly level, so it makes system administrator to analyse logs of the most suspected users first.

TABLE 1:
INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING

Therefore our method provides high speed of detecting attacks. We are suggested to generate a multi hop cloud network. First we are going to connect the network. each node is connected the neighboring node and it is independently deployed in network area when a packet is generated by the sender the packet get activated .The authenticated user to allow accessing a cloud space for storing or retrieving a file or any application. Cloud networks which generate security event and alerts and control the cloud networks. After this, browse and select the source files and selected data is converted into fixed size of packet and the packet is send from source to destination. Monitoring and analyzing by genetic Algorithm the event occurring in the network in order to detect abnormal activities through genetic algorithm. The intrusion detection is defined as a mechanism for a packet in network to detect the existence of inappropriate, incorrect, or anomalous moving attackers. If the Genetic Algorithm found an anomalous behavior then the packet will be blocked. After filtering the invalid packets will be block and all the valid Packets will reach to the destination. There are several ways to categorize IDS depending on the type and location of the cloud networks and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance. J. H. Lee et al. has proposed a novel approach to detect intrusions based on the anomaly level of users for efficient utilization of resources [21]. The main component of the proposed system is authentication, authorization and accounting (AAA) module. When a user attempts to use cloud services, he is authenticated using AAA module. Upon successful authentication, the anomaly level of user is retrieved which is based on recent information about the user in the database. Consequently, AAA selects the appropriate IDS having security level relevant to the anomaly level of user. The selected IDS is deployed in host operating system (OS) and AAA asks it to assign guest OS for the user. When a guest OS is assigned to the user, a connection is set up between the guest OS and user data in storage center. The security levels of IDS are: High which includes all known attack patterns and a fraction of anomaly method where more security is needed, medium which provides somewhat strong security using all known attack patterns and low which makes use of selected known attack patterns that are more malicious, have high rate of occurrence and cause severe damages to system. So, the proposed method provides high speed of detecting attacks and more guest OS can be assigned since medium-level and low-level IDS use less resources. The proposed system also facilitates the system administrators by letting them audit the logs based on the anomaly level of users. A.V. Dastjerdi et al. has proposed and implemented an intrusion detection system (IDS) which utilizes mobile agents (MA) to detect intrusions in cloud environment [22].

TABLE 2
IDS MODELS & CLASSIFICATIONS FOR CLOUD COMPUTING ENVIRONMENT

Reference	Solution	Remark
Roberto Di Pietro and Luigi V. Mancini [28]	Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer.	Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server Based Computing(SBC), and Network Computing, rather than entirely new type of computing technique
JaeHyuk Jang, Cisco, [29]	Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer.	Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server Based Computing(SBC), and Network Computing, rather than entirely new type of computing technique[
Roschke and Cheng et al. [2]	central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface	Providing a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user.
Parag K. Shelke, [5]	providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission	Our proposed cloud IDS handles large flow of data packet, analyze them and generate reports efficiently by integrating knowledge and behavior analysis to detect Intrusion.
S. N. Pawar. [7]	Intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks.	A number of soft computing based approaches are being used for detecting network intrusion
Monjur ahmed and mohammad ashraf hossain, [9]	Security issues in cloud computing.	If security is not robust and consistent, the flexibility, and advantages that cloud computing has to offer will have little credibility
M. S. hoque, et al. [10]	Nowadays it is very important to maintain a high level security to ensure safe and trusted communication of information between various organizations.	An implementation of intrusion detection system using genetic algorithm,

In the proposed model, each subnet of virtual machines (VM) contains an IDS which comprises four main modules: An agency that provides an environment to execute MAs. Static Agent Detector which observes the VMs and upon detection of some suspicious activity, it generates alert, logs information about it and sends alert ID to IDS Control Center (IDS CC). Then, IDS CC sends investigative MAs (IMA) to each agency that generated similar alerts. Each IMA can detect some particular intrusions. The task of IMA is to collect the proofs of an attack for further analysis by visiting all VMs and send the information back to IDS CC. Here, the alerting console compares the doubtful activity with a database of intrusions located in IDS CC and raises an alarm if match is found. A blacklist of all compromised VMs containing their names and identification is sent to all VMs apart from blacklisted VMs. There are three possible types of VM in proposed system: normal, compromised, and migrated. In order to stop propagation of intrusions, compromised VMs must be banned from migration. The proposed model provides high flexibility and scalability by using MAs. It can detect even new attacks using data mining technique. Attacks on IDS CC are detectable using P2P model. However, when compared to client/server approach, the number of VMs to visit is limited to 6 hosts, and if the limit is exceeded, the network load starts increasing than for client/server design. S. Bharadwaja et al. [25] has proposed a Virtual Machine Monitor (VMM) based technique to detect intrusions in a virtualized environment. The system "Collabra" is integrated with each VMM and acts as an interface between Dom0 of Xen based virtual network and VMM. It monitors the hyper-calls from guest Virtual Machines (VMs) to VMM and analyzes them for anomalies. The reason for using anomaly based detection method is lack of any familiar hyper-call attacks that can be used as signatures. So it can effectively detect unknown attacks. The system works in a collaborative manner since it can communicate with all instances of itself that are deployed on different VMMs. If an intrusion is detected, it instantly uses logical domain channels (LDC) to inform other instances about the features of attack and calls for sanitizing the particular VMM. The hyper-calls are classified as being normal or anomalous based on a threshold value. Collabra system provides two main security components: hyper-call integrity check where Collabra performs cross verification of each hyper-call initiated by a guest VM based on a message authentication code (MAC) and
a specific policy for that call. The MAC is helpful in maintaining the integrity of a hypervisor based VM network. The hyper-call origin access where the origin of legitimate hyper-calls is identified by admin version of Collabra. Hyper-calls invoked by locations other than valid applications of guest VMs are marked as untrusted and the related instance of Collabra is informed about the details of such calls. The proposed system can detect collaborative and distributed attacks at the hypervisor layer in real time.

Models	Category	Remark
C. C. Lo, C. C. Huang, J. Ku [16]	Signature Based IDS	Proposed and simulated an IDS that works in cooperative way to counter the DoS and DDoS attacks.
Mazzariello et al.[18.	Signature Based IDS	Tested the deployment of IDS at various positions in cloud to detect DoS attacks on virtual SIP-based hosts].
Bakshi et al. [19]	Signature Based IDS	Proposed and implemented a solution for detection of DDoS attacks
Patel et al. [20]	Anomaly Based IDS	Proposed an autonomic agent-based intrusion prevention system using the principles of autonomic computing
J. H. Lee et al. [21].	Anomaly Based IDS	Proposed a novel approach to detect intrusions based on the anomaly level of users for efficient utilization of resources
A.V. Dastjerdi et al. [22].	Anomaly Based IDS	Proposed and implemented an intrusion detection system (IDS) which utilizes mobile agents (MA) to detect intrusions in cloud environment
S. Bharadwaja et al. [25]	Anomaly Based IDS	Proposed a Virtual Machine Monitor (VMM) based technique to detect intrusions in a virtualized environment
Ms. Parag K. Shelke et al [26].	Hybrid IDS	Proposed a multi-threaded NIDS to solve the problem of Cross Site Scripting (XXS) and DDoS attacks
K. Viera et al. [23].	Hybrid IDS	Proposed an Intrusion Detection System for Grid and Cloud Computing (GCCIDS) that works at middleware layer and can detect particular intrusions by using a combination of knowledge-based and behavior-based techniques
C. N. Modi et al. [17].	Hybrid IDS	Proposed and implemented a Network IDS which uses Snort to detect known attacks and Bayesian classifier to detect unknown attacks.
S. N. Dhage et al. [24]	Hybrid IDS	Proposed an IDS scheme in which the IDS controller deploys a separate instance of IDS between the user and cloud service provider when any user needs to access a cloud service

4.3 Hybrid IDS: Ms. Parag K. Shelke et al has proposed a multi-threaded NIDS to solve the problem of Cross Site Scripting and DDoS attacks [26]. The proposed NIDS consists of three components each performing a specific role: The capture module collects the incoming and outgoing packets (UDP, TCP, ICMP, IP) and transmits to a common queue for evaluation. The analysis and processing module evaluates the received data packets by matching them against a knowledge base and a predefined set of rules. The multi-threaded processes in shared queue boost the performance of NIDS. The effective matching and evaluation helps in identification of malicious packets and alert generation. The reporting module generates alert reports based on information from shared queue. The third party service observing the entire scenario, instantly informs user about the attack details and provides a consultative report to the service provider. Although it is a novel approach however, the implementation details are not provided to prove the concept. K. Viera et al. has proposed an Intrusion Detection System for Grid and Cloud Computing (GCCIDS) that works at middleware layer and can detect particular intrusions by using a combination of knowledge-based and behavior-based techniques [23]. In this system, every node can identify intrusions and generates alerts for other nodes. So intrusion detection process takes place in a cooperative manner. The four major components of the proposed architecture other than IDS service are: the node containing resources to be accessed equally through middleware, the service which helps in communication, the event auditor which collects data from different sources like service, log system, and node messages. The fourth component is the storage service which stores data to be analyzed by IDS service. The authors have evaluated the behavior-based system by measuring false positives and false negatives and concluded that false negatives are always more than false positives when same amount of data is used as input. On the other hand, they have evaluated the knowledge-based system by using audit data from log system and the communication system and concluded that it is possible to analyze the traffic in real-time if limited number of rules are used for comparison. K. Viera et al. has not given implementation details, however they intend to implement it in their future work. In order to tackle both known and unknown attacks, C. N. Modi et al. has proposed and implemented a Network IDS which uses Snort to detect known attacks and Bayesian classifier to detect unknown attacks [17]. The major components of the proposed system are: Packet Preprocessing, which takes network packets and eliminates the information that does not associate to detection. Analyzer, comprising Bayesian classifier, Snort, and Alert Log, uses signature based or anomaly based detection method to evaluate the packet as being normal or intrusion and if it is an intrusion, records the intrusion using Alert Log and notifies NIDS on other servers which store it in their storage. The Knowledge base and Behavior base present in Storage module, store rules of known attacks and normal/intrusion network events respectively. When network packets are captured, first of all, Snort is used for detection and intrusion events are stored in alert database. Next, anomaly detection is performed by first preprocessing the non-intrusion packets and then using Bayesian classifier to calculate their class label (intrusion or normal) by keeping in view the behavior base and finally logging the calculated intrusions into alert database. NIDS set up in all servers work in a collaborative manner by adding the alerts into their knowledge base and thus making detection of unknown attacks easier. In this technique, signature based detection is followed by anomaly based detection, resulting in better detection time since anomaly detection technique detects just unknown attacks. Moreover, detection rate is improved by sending alert to other NIDS deployed in cloud environment. S. N. Dhage et al. [24] has proposed an IDS scheme in which the IDS controller deploys a separate instance of IDS between the user and cloud service provider (CSP) when any user needs to access a cloud service. IDS instance observes all activities of the user and sends a log of complete session to IDS controller. This information is used to maintain samples of user's activities which are stored in Knowledge Base and help IDS controller in identification of that user on next session and detection of intrusions since Knowledge Base can also discover new samples using neural networks. Different users may also be assigned IDS having different set of rules according to the requirements of each user. The IDS instance should be installed on each layer of cloud i.e. system, platform and application. The proposed intrusion detection techniques include; Signatures, several incorrect passwords for an account, violation of Access rights, and many more. The proposed IDS is able to detect unknown attacks using neural networks, however it is a theoretical model and authors intend to implement it using Eucalyptus cloud.

5. BEST OPEN SOURCE SIMULATOR FOR CLOUD COMPUTING

5.1 CloudSim [31]**:** is a new, highly generalized and extensible Java based simulation tool kit, and is actually regarded as a software framework. It supports several core functionalities like queuing and processing of events, the creation of CloudSim entities, communication among components and the management of the simulation clock. CloudSim has been developed by the CLOUDS Laboratory of the Computer Science and Software Engineering Department of the University of Melbourne, Australia by Prof. (Dr) Rajkumar Buyya. This tool kit enables seamless modelling, simulation and experimentation in cloud computing and application services. It can be termed as 'running a model of

an environment by taking the hardware as base, where technology-specific details are abstracted. CloudSim features include basic classes for deriving data centres, virtual machines, applications, users, computational resources, and policies for managing diverse parts of the system like scheduling and provisioning. It implements general application provisioning techniques, which can be extended easily with minimal effort.
The latest version of CloudSim is 4.0. Its features are listed below:

a. Supports modelling and simulation of large scale cloud computing data centers.
b. Supports modelling and simulation of virtualized server hosts, along with customizable policies for provisioning host resources to virtual machines.
c. Supports dynamic inclusion of simulation elements, discontinuations and restarts.
d. Has support for user defined policies for allocating hosts to virtual machines (VMs).
e. Supports the creation of various data center network topologies, message-passing applications and energy-aware computational resources.
f. Has the capability to simulate a federated cloud environment that inter-networks resources from both private and public domains. This is a critical feature for research into cloudbursts and automatic application scaling.

5.2 CloudAnalyst [31]**:** A GUI based simulator derived from CloudSim, has some extended features and capabilities. CloudAnalyst was proposed by Bhathiya W. and Rajkumar B. at the CLOUDS Laboratory of the Computer Science and Software Engineering Department of the University of Melbourne, Australia. The simulator supports the evaluation of social network tools according to the geographical distribution of users and data centres. It can be applied to determine the behavior of large scale Internet applications in the cloud, and also enables a modeler for looping simulations and to conduct a series of simulations with slight variations in parameters. CloudAnalyst is regarded as a powerful simulation framework for deploying real-time data centres and monitoring load balancing, cloud cluster monitoring and data centre data flow in real-time. It allows users to save simulation configurations as XML files and exports live results in PDF format. The features of CloudAnalyst are listed below.

a. ***Graphical user interface:*** Easy-to-use GUI for setting up and viewing results of all sorts of cloud computing experiments.
b. **Simulation definition via a high degree of configuration and flexibility:** CloudAnalyst is equipped with modelers that have a high degree of control over the experiment by modelling entities such as data centres, virtual machines, memory, storage and bandwidth.
c. **Experiment looping:** CloudAnalyst can save simulation scenarios and loop them again and again via simulation variations. It can save the results as XML files and even save PDF files of the results.
d. **Efficient output:** CloudAnalyst provides graphical output of simulation results in the form of tables and charts, apart from a large amount of statistical data.

5.3 GreenCloud [31]**:** provides a simulation environment for energy-aware cloud computing data centres. It is regarded as the most sophisticated packet-level simulator available till date for energy-aware cloud computing data centres, with a focus on cloud communications. It offers a detailed fine-grained modelling of the energy consumed by the data centre's IT equipment such as computing servers, network switches and communication links. The GreenCloud simulator was developed by Dzmitry Kliazovich (Project Leader), research fellow at the Faculty of Science, Technology and Communication of University of Luxembourg with other team members. This simulator is used to develop novel solutions in monitoring, resource allocation, workload scheduling as well as communication protocols, optimization and network infrastructure.
GreenCloud has been developed as an extension of the NS-2 packet-level network simulator. It distinguishes between three energy consumption components—computing energy, communicational energy and energy components related to the physical infrastructure of a data centre. The latest version of GreenCloud is 2.1.2. The features of GreenCloud simulator are listed below:

a. The simulator mainly focuses on the cloud network and, particularly, energy consumption monitoring in cloud computing technologies.
b. It supports simulation of CPU, memory, storage and networking resources.
c. Supports researchers in exploring methods to minimize electricity consumption by improving power management, as well as dynamically managing and configuring the power-aware capability of the system's devices.
d. Has a user-friendly GUI and is open source.

5.4 iCanCloud [31]**:** is a cloud computing simulation platform which is based on SIMCAN and supports the simulation of large storage networks. The iCanCloud simulation framework was developed by A. Nunez and J.L. Vazquez-Poletti with the objective of predicting the trade-offs between cost and performance of a given set of applications executed in specific hardware. The simulator then provides users information about such costs. iCanCloud was designed to optimise flexibility, accuracy, performance and scalability, and has turned into a powerful simulator for designing,

testing and analysing all sorts of existing and non-existing cloud architectures. iCanCloud is being developed over the OMNeT++ platform. The latest version is 1.0 and requires OMNeT++ 4.6 and INET 2.5. It can be installed on all versions of Ubuntu and on MAC platforms. The features of iCanCloud are listed below:

a. Both existing and non-existing cloud computing architectures can be modelled and simulated.
b. A flexible cloud hypervisor module provides an easy method for integrating and testing both new and existent cloud brokering policies.
c. Customisable VMs can be used to quickly simulate uni-core/multi-core systems.
d. iCanCloud provides a wide range of configurations for storage systems, which include models for local storage systems, remote storage systems like NFS, and parallel storage systems (like parallel file systems and RAID systems).
e. iCanCloud provides a user-friendly GUI that makes it easier to generate and customise large distributed models. This GUI is especially useful for managing a repository of preconfigured VMs, a repository of preconfigured cloud systems, and a repository of preconfigured experiments to launch experiments from the GUI and generate graphical reports.
f. iCanCloud provides a POSIX-based API and an adopted MPI library for modelling and simulating applications. Also, several methods for modelling applications can be used in iCanCloud—using traces of real applications, using a state graph, and programming new applications directly in the simulation platform.
g. New components can be added to the repository of iCanCloud to increase its functionality.

5.5 EMUSIM [31]**:** stands for Integrated Emulation and Simulation. It combines emulation (AEF-Automated Emulation Framework) and Simulation (CloudSim) to enable more accurate models of software artefacts to be used during simulations. EMUSIM was developed by Rodrigo N. Calherios at the Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, University of Melbourne, Australia. EMUSIM automatically extracts information about application behaviour via emulation and then uses this information to generate a corresponding simulation model. The EMUSIM simulator is of great use when the tester has no idea about the performance of the software under the varied levels of concurrency and parallelism which impede simulation. These can replace *in-site* experiments that would require infrastructure that is either unavailable for the tester or too expensive to run in the public cloud. EMUSIM is open source software under the GPL License. The latest version of AEF is 1.3, released in August 2010. The features of EMUSIM are listed below:

a. Offers a combination of simulation and emulation to evaluate the effect of varying resources and patterns of requests on cloud applications.
b. Accurately models applications to supply information regarding performance.
c. Reduces the cost of running cloud based simulation, because rather than local and limited infrastructure usage, a pay-as-you-go public cloud is used for evaluation purposes.
d. Supports loosely coupled CPU-intensive applications.

5.6 GroudSim (Gr-Grid oud-Cloud) [31]**:** is an event-based simulator designed for scientific applications on grid and cloud environments. It only requires one simulation thread. GroudSim was developed by S. Ostermann, K. Plankensteiner and D. Bodner, and can also be termed as a grid and cloud simulation tool kit for scientific applications based on a scalable simulation-independent discrete-event core. GroudSim provides a comprehensive set of features for complex simulation scenarios, ranging from simple job executions on leased computing resources to calculation of costs, and background load on resources. GroudSim mainly focuses on the IaaS area of cloud computing. It can be easily extended to additional models like SaaS and PaaS in cloud computing.

SimEngine is the main class of GroudSim, which implements the time advance algorithm, the clock and the future events list, keeping track of the registered entities used for tracing during a simulation. The grid and cloud resources classes share most of the common functionality implemented in the Groud package and override the specialised behaviour in the Groud.

The features of GroudSim are listed below:

a. It is a powerful Java based simulation tool kit for scientific applications. It combines grid and cloud infrastructures, and is based on a discrete-event simulation tool kit.
b. Improvised performance as compared to process based approaches in other simulators.
c. Can be extended easily by adopting probability distribution packages.
d. The most unique feature in GroudSim is GroundEntity, which has its own definition for error behaviour. The user can change this configuration during each error occurrence.

5.7 DCSim (Data Centre Simulation) [31]**:** DCSim is regarded as an extensible data centre simulator designed in Java. It provides a stable and easy framework for developing and performing high-end experiments on data centre management techniques and algorithms. DCSim, being an event-driven simulator, simulates a data centre IaaS offering

to multiple clients. DCSim provides the additional capability of modelling replicated VMs, sharing incoming workloads as well as dependencies between VMs that are part of a multi-tiered application. The features of DCSim are listed below:

a. Contains a multi-tier application model that allows the simulation of dependencies between VMs.
b. Facilitates rapid development, evaluation and feedback on data centre management policies and algorithms.

6. STATE OF THE ARTS INDUSTRIALIZED CLOUD SERVICE PROVIDERS

The importance of Cloud computing and its future you can predict on the basis of that almost all big-players in the software industry are deploying their cloud services. The future of any technology depends upon the condition that how much industrialization is going on for that technology.

Microsoft [32] Azure has four features in its cloud; its deep involvement at all three layers of the cloud (IaaS, PaaS and SaaS); its unmatched commitment to developing and helping customers deploy Artificial Intelligence, Machine Learning and Blockchain in innovative production environments;

Amazon Web Services (AWS) [32] is effectively documented, seamless integration and has the most widespread tools and services available. AWS is good for cost effective for business operations and high scalability and availability.

IBM [32] plays in all three layers IaaS, PaaS and SaaS which is hugely important for the elite cloud vendors because it allows them to give customers more choices, more seamless integration, better cybersecurity, and more reasons for third-party developers to rally to the IBM Cloud. Plus, its relentless pairing of "cloud and cognitive" is an excellent approach toward weaving Artificial Intelligence and Machine Learning deeply into customer-facing solutions.

Google Cloud Platform GCP [32] is known for power and simplicity. It is good for the developers who seeks for streamlined eco-cloud system for development and deployment.

SAP [32] is able to play nice in heterogeneous environments. Plus, SAP's HANA technology is now in full deployment across thousands of businesses, and as it takes root and SAP continues to rationalize its massive product portfolio around HANA in the cloud, SAP has a very bright future ahead of it in the cloud.

Oracle Cloud OC [32] has increased business agility, lower costs and reduced complexity. It has enterprise grade cloud computing capabilities with SaaS, PaaS, and IaaS.

7. CONCLUSION

Cloud computing is a "network of network" over the internet, therefore chances of intrusion is more with the erudition of intruder's attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For cloud computing, enormous network access rate, relinquishing the control of data and application to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this paper, a multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user And also have surveyed the state-of-the-art of cloud computing, covering its essential concepts, architectural designs, prominent characteristics, key technologies as well as research directions. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

REFERENCES

[1] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," Computers & Security, vol. 30, pp. 719-731, 2011.

[2] Sebastian Roschke, Feng Cheng, Christoph Meinel," Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[3] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", Special Publication 800-145, Sep. 2011.

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

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

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

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

[8] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, "A Survey of Intrusion Detection Techniques in Cloud", Journal of Network and Computer Applications 36 (2013), pp. 42–57.

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

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

[11] Kleber, schulter, "Intrusion Detection for Grid and Cloud Computing", IEEE Journal: IT Professional, 19 July 2010.

[12] U. Oktay, O. K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing", ISBN: 978-1-4673-5613-8, 2013, IEEE, pp. 98-104.

[13] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," NIST Special Publication, vol. 800, p. 94, 2007.

[14] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," Information Management & Computer Security, vol. 18, pp. 277-290, 2010.

[15] A. Patel, M. Taghavi, K. Bakhtiyari, J. C. Ju´nior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview", Journal of Network and Computer Applications 36 (2013), pp. 25–41.

[16] C. C. Lo, C. C. Huang, J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops 2010, pp. 280-284.

[17] C. N. Modi, D. R. Patel, A. Patel, R. Muttukrishnan, "Bayesian Classifier and Snort based Network Intrusion Detection System in Cloud Computing", Third International Conference on Computing, Communication and Networking Technologies, 26th-28th July 2012.

[18] C. Mazzariello, R. Bifulco and R. Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment", 2010 Sixth International Conference on Information Assurance and Security, pp. 265-270.

[19] A. Bakshi, Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine", 2010 Second International Conference on Communication Software and Networks, pp. 260-264

[20] A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior and C. Wills, "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System", Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), pp. 223-234.

[21] J. H. Lee, M. W. Park, J. H. Eom, T. M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", ICACT, 2011, pp. 552-555.

[22] A. V. Dastjerdi, K. A. Bakar, S. G. H. Tabatabaei, "Distributed Intrusion Detection in Clouds using Mobile Agents", Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, pp. 175-180.

[23] K. Vieira, A. Schulter, Carlos B. Westphall, and C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing", IEEE Computer Society, (July/August 2010), pp. 38-43.

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

[25] S. Bharadwaja, W. Sun, M. Niamat, F. Shen, "Collabra: A Xen Hypervisor based Collaborative Intrusion Detection System", Eighth International Conference on Information Technology: New Generations, 2011, pp. 695-700.

[26] Ms. P. K. Shelke, Ms. S. Sontakke, Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012, pp. 67-71.

[27] Ku. Shraddha D. Patil," To Implement Intrusion Detection System for Cloud Computing Using Genetic Algorithm", International Journal of Computer Science and Information Technology Research ISSN 2348-120XVol. 3, Issue 1, pp: (193-198), Month: January - March 2015, Vol. 3, Issue 1, pp: (193-198), Month: January - March 2015,

[28] Roberto Di Pietro and Luigi V. Mancini, Intrusion Detection Systems, Springer, Jan. 2008.

[29] JaeHyuk Jang, Cisco, Cloud Computing: Drive Business Paradigm Shift, 2010.

[30] R.hangsman and mark spenson, —advanced security concepts on data management,‖ technology, vol,326,apr 2009, pp. 1076-1128.

[31] Anand Nayyar"Best Open Source cloud computing simulator" article published in opensource forum in November 2016. http://opensourceforu.com/2016/11/best-open-source-cloud-computing-simulators/

[31] S. Kamboj and N. S. Ghumman, "A survey on cloud computing and its types," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 2971-2974.

[32] **Bob Evans**," The Top 5 Cloud-Computing Vendors", https://www.forbes.com/sites/bobevans1/2017/11/07/the-top-5-cloud-computing-vendors-1-microsoft-2-amazon-3-ibm-4-salesforce-5-sap/#30ccdf226f2e

Mr. Mohammad Yesuf Getu is working in the Samara University (Ethiopia) in the capacity of Lecturer in the department of Computer Science. He completed his Masters in Computer Application from Andhra University (India) and Masters in Information Technology from Alagappa University (India). He is also serving the Samara University in the position of Registrar since 2014. His Research Interest is Cloud Computing and Artificial Intelligence.

Dr. Shahnawaz Husain is working in Samara University, Ethiopia in the capacity of Assistant Professor in the department of Computer Science. He completed his Ph.D (C.S&E) in broad area of network security. He was the alma-mater of King Khalid University (K.S.A), Graphic Era University (India) and Jamia Millia Islamia, New Delhi (India). He published more than fifty research article in various international journals and conferences of repute. His research interest is Computer Networks & Security.