International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 619 - 624

Cloud Computing Security and Issues

Sandesh Bagade
Department of Computer Engineering
University of Mumbai
ARMIET, Shahapur, India
sandesh.bagade@gmail.com

Ravi Rane
Department of Computer Engineering
University of Mumbai
DRIEMS, Neral, India
ravirane143@gmail.com

Prof. Ankush Pawar
Department of Computer Engineering
University of Mumbai
DRIEMS, Neral, India
ankushpawar1981@gmail.com

Abstract **-** Cloud computing is architecture for providing computing service via the internet on demand and pay per user access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Cloud security is becoming a key differentiator and competitive edge between cloud providers. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing.

Index Terms **-** *Cloud, Security, Security challenges, Cloud computing.*

*****

I. INTRODUCTION

The expression "cloud" was authored from the PC system graphs which utilize it to shroud the intricacy of base included. Distributed computing gives programming, stage and foundation as an administration. Its principle highlights incorporate asset pooling, quick versatility, measured administration, on-interest self-administration and expansive system access. Along these lines, a cloud is an accumulation of equipment and programming that keeps running in a server farm and empowers the distributed computing model. A cloud lessens capital speculation, equipment expense and programming permit cost. Distributed computing likewise raises extreme difficulties particularly with respect to the security level required for the protected utilization of administrations gave by it. There are no publically accessible measures particular to distributed computing security. Thus, in this paper, we propose the accompanying measures for keeping up security in a risky distributed computing environment. Clouds are broadly classified as:

1. **PERSONAL CLOUDS**: Such clouds are especially operated by single organization.
2. **GENERAL CLOUDS**: These clouds are used for providing services to common people
3. **DOMAIN-SPECIFIC CLOUDS**: These clouds are maintained for specific requirements by a group of organizations.
4. **MIXED CLOUDS**: These clouds are mixtures of above said three clouds which can share data to achieve fulfil a specific requirement [2].

II. CLOUD COMPUTING BUILDING BLOCKS

A. Different models of cloud computing

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1].

1. ***Software-as-a-Service (SaaS):*** SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support [5]. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data centre space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

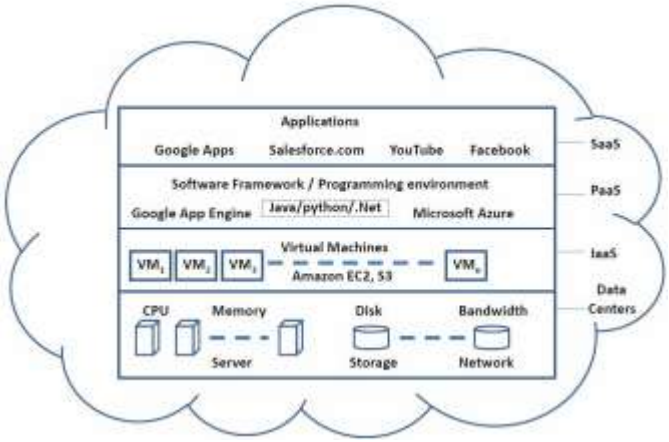

Figure 1. High Level View of Cloud Computing Architecture

2. ***Platform as a Service (PaaS)****:* "PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating

systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

3. ***Infrastructure as a Service (IaaS):***

Infrastructure as a service (IaaS) alludes to the sharing of equipment assets for executing administrations utilizing Virtualization innovation. Its primary goal is to make assets, for example, servers, system and capacity all the more promptly available by applications and working frameworks. In this way, it offers fundamental framework on-interest administrations and utilizing Application Programming Interface (API) for collaborations with hosts, switches, and switches, and the ability of including new gear in a basic and straightforward way. As a rule, the client does not deal with the basic equipment in the cloud foundation, however he controls the working frameworks, stockpiling and sent applications. The administration supplier claims the gear and is in charge of lodging, running and looking after it. The customer normally pays on a for every utilization premise. Case of IaaS incorporate Amazon Elastic Cloud Computing (EC2), Amazon S3, and Go Grid.

B. *Cloud computing entities*

Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows,

Cloud Providers: Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers [6].

Cloud Service Brokers: Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

Cloud Resellers: Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed [7].

III. CLOUD COMPUTING INFRASTRUCTURE

Figure 2 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture.

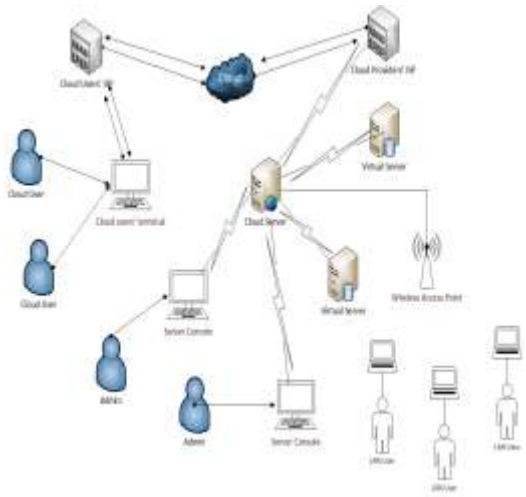

Figure 2: A Typical Cloud Architecture

The representation of cloud engineering in figure 2 is a most straightforward one where couple of complex qualities of distributed computing (e.g. repetition, server replication, and geographic scattering of the cloud suppliers' system) are not demonstrated – the reason for the outline is to set up the game plan that makes the idea of distributed computing an unmistakable one. The system design is clear as crystal with the distinguishing proof of cloud clients when considered in-accordance with the examination of the distributed computing idea introduced before. One prominent part from the design is that, while the cloud clients are unmistakably distinguished and named appropriately because of their remote area and method for remote access to the cloud servers, the administrator clients who are controlling the cloud servers are not cloud clients in any structure as for the cloud administration supplier's system in the situation. It is doubtful whether the LAN clients in figure 2 are cloud clients or not. Such space for contention could exist because of the expression 'distributed computing' being an idea instead of a specialized wording. On the off chance that the meaning of distributed computing is taken to have vital game plans of being the servers found remotely that are gotten to through open framework (or through cloud), then the LAN clients in figure 2 may not be considered as the cloud clients in the connection. Concerning circulated and lattice processing as the mother innovation that characterize the infrastructural way to deal with accomplish distributed computing, the LAN clients in the situation are basically the cloud clients when they utilize the cloud administrations offered by the servers; the LAN clients in this point of view are basically utilizing assets that are "obtained" from the servers on an on-interest premise.

Figure 3 illustrates the hierarchical arrangement based on which a cloud is perceived in the form of IaaS, PaaS and SaaS from any cloud end-user's viewpoint.

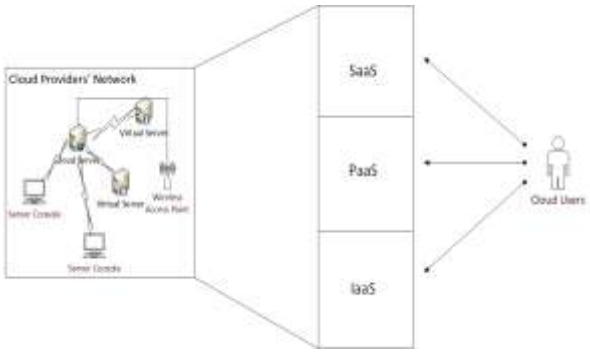

Figure 3: Cloud Service Hierarchy

As depicted in figure 3, the technical details, arrangements and management of the cloud service providers' network is transparent to the cloud user. From the end of the cloud user, the service from the provider comes in the form of SaaS, PaaS or IaaS where the cloud user has no intention or worry about what goes on in the internal arrangement of the cloud service providers' network. Any disruption of any form for whatever is the reason, deem to the cloud users either as service unavailability or quality deterioration – its affect and ways to counter this disruption is a critical part for the cloud infrastructure. Security issues might play a stimulating role as a driving factor for any aforementioned disruption.

IV. AUTHENTICATION IN CLOUD

Security is the most prioritized aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well. As the cloud computing approach could be associated with having users' sensitive data stored both at clients' end as well as in cloud servers, identity management and authentication are very crucial in cloud computing. Verification of eligible users' credentials and protecting such credentials are part of main security issues in the cloud - violation in these areas could lead to undetected security breach at least to some extent for some period. A possible authentication scenario for a cloud infrastructure is illustrated in figure 4.

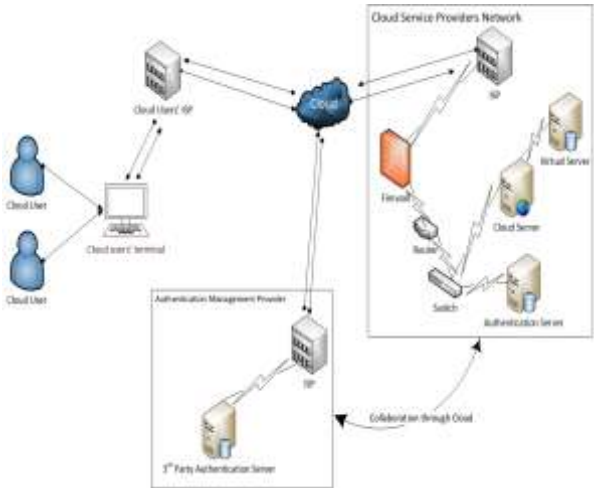

Figure 4: Authentication in the Cloud

The delineation exhibited in figure 4 passes on that the confirmation for the cloud clients should be possible either by the cloud administration supplier or the administration supplier can outsource the personality administration and verification administration to outsider experts. In the later case, the cloud administration supplier is required to have joint effort with the outsider validation master – the cooperation between the cloud administration supplier and the outsider confirmation authority amid the verification procedure of cloud clients is done basically through cloud. This element includes execution overheads and security issues to the cloud setting as the message going between outsider validation administration power and the cloud administration supplier as a major aspect of joint effort may basically be done through cloud foundation. As examined before, the aggregate verification procedure and how they are completed - paying little heed to the association of outsider validation experts – is straightforward to the cloud clients. The delineation on the confirmation situation displayed above is a genuinely basic one – if topographically scattered servers are conveyed by the cloud administration suppliers then the aggregate verification procedure may be significantly more intricate as far as security, fundamental calculation and additionally execution level. Whatever is the level of intricacy, the presentation of outsider validation and personality administration expert into any cloud engineering ought to have one and only objective; and the objective is to fortify the vigor of security in the concerned zone which the cloud administration supplier itself is not equipped for to send or offer.

V. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy

- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Access to Servers & Applications: In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which are not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users [8].

Most companies are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest cloud application adoption rate, Active Directory (AD) seems to be the most popular tool for managing users. With cloud application, the software is hosted outside of the corporate firewall. Many times user credentials are stored in the cloud application provider's databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple cloud application products will increase IT management overhead. For example, cloud application providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users. Large enterprises, the management of user's account as the adoption of single sign on (SSO) or each employee will be dispatched some different accounts to access different systems. Thus, multi-authentication for each employee might be very often to be confronted in an enterprise. Those accounts that come along with each individuals might be the same or different. Therefore, how could the administrator well manage those user's identification accounts and the corresponding passwords or achieve the state of SSO is another important issue. Nevertheless, the application of SSO for identification and authentication does have serious information security risk. In addition, the management of authorized access privilege is also a critical key point.

Data Transmission: Encryption strategies are utilized for information as a part of transmission. To give the insurance to information just goes where the client needs it to pass by utilizing verification and respectability and is not changed in transmission. SSL/TLS conventions are utilized here. In Cloud environment the vast majority of the information is not encoded in the preparing time. However, to process information, for any application that information must be decoded. In a completely homomorphism encryption plan advance in cryptography, which permits information to be prepared without being decoded. To give the privacy and uprightness of information in-transmission to and from cloud supplier by utilizing access controls like approval, validation, evaluating for utilizing assets, and guarantee the accessibility of the Internet-confronting assets at cloud supplier. Man-in-the-center assaults is cryptographic assault is completed when an assailant can put themselves in the correspondence's way between the clients. Here, there is the likelihood that they can hinder and change correspondences.

Virtual Machine Security: Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems. VMM (Virtual Machine Monitor) is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability was found in VMware's shared folders mechanism that grants users of a guest system read and writes access to any portion of the host's file system including the system folder and other security-sensitive files. Vulnerability in Xen can be exploited by "root" users of a guest domain to execute arbitrary commands. The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual Machine Monitor) do not offer perfect isolation. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system.

Network Security: Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems.

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network.

Reused IP address issues have been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

Data security: For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party.

Data Privacy: The information protection is additionally one of the key attentiveness toward Cloud figuring. A protection directing panel ought to likewise be made to settle on choices identified with information security. Necessity: This will guarantee that your association is set up to meet the information protection requests of its clients and controllers. Information in the cloud is normally comprehensively circulated which raises worries about ward, information introduction and protection. Associations stand a danger of not consenting to government approaches as would be clarified further while the cloud sellers who uncover delicate data hazard legitimate risk. Virtual co-tenure of delicate and non-touchy information on the same host additionally conveys its own particular potential dangers.

Data Integrity: Information debasement can happen at any level of capacity and with a media, So Integrity checking is vital in distributed storage which is basic for any server farm. Information trustworthiness is effortlessly accomplished in a standalone framework with a solitary database. Information uprightness in such a framework is kept up through database imperatives and exchanges. Exchanges ought to take after ACID (atomicity, consistency, seclusion and solidness) properties to guarantee information uprightness. Most databases bolster ACID exchanges and can protect information uprightness. Information produced by distributed computing administrations is kept in the mists. Keeping information in the mists implies clients may lose control of their information and depend on cloud administrators to uphold access control.

Data Location: As a rule, cloud clients don't know about the careful area of the datacenter furthermore they don't have any control over the physical access components to that information. Most surely understood cloud administration suppliers have datacenters around the world. In numerous a cases, this can be an issue. Because of consistence and information protection laws in different nations, region of information is of most extreme significance in numerous endeavor designs. For instance, in numerous EU and South America nations, certain sorts of information can't leave the nation as a result of conceivably delicate data. Notwithstanding the issue of nearby laws, there's likewise the subject of whose purview the information falls under, when an examination happens. Next in the unpredictability chain are appropriated frameworks. In a dispersed framework, there are numerous databases and different applications [9].

V. RESEARCH CHALLENGES IN CLOUD COMPUTING

Cloud Computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures, also the challenges of allowing

applications and development platforms to take advantage of the benefits of cloud computing. The research on cloud computing is still at an early stage. Many existing issues have not been fully addressed, while new challenges keep emerging from industry applications. Some of the challenging research issues in cloud computing are given below.

- Service Level Agreements (SLA's)
- Cloud Data Management & Security
- Data Encryption
- Migration of virtual Machines
- Interoperability
- Access Controls
- Energy Management
- Multitenancy
- Server Consolidation
- Reliability & Availability of Service
- Common Cloud Standards
- Platform Management.

VI. CONCLUSIONS

One of the greatest security stresses with the distributed computing model is the sharing of assets. Cloud administration suppliers need to illuminate their clients on the level of security that they give on their cloud. In this paper a great part of the work has been centered around sorts of mists and their security difficulties and it depicts the method for planning the answer for the security dangers. It gives a correlation between various administrations suppliers on various cloud administrations SaaS, PaaS, IaaS. This audit demonstrates that there are a few sorts of mists and the related security challenges on every level.

REFERENCES

[1] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges" IJCSITS, Vol. 1, No. 2, December 2011.

[2] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma " Cloud Computing: Different Approach & Security Challenge" International Journal of Soft Computing and Engineering.

[3] (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012 421 Monjur Ahmed and Mohammad Ashraf Hossain "Cloud Computing and Security Issues in the Cloud" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 DOI : 10.5121/ijnsa.2014.6103 25.

[4] Pankaj Arora* Rubal Chaudhry Wadhawan Er. Satinder Pal Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[5] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[6] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[7] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[8] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695- 3929 -4.

[9] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.