INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

CLOUD COMPUTING AND SECURITY ISSUES IN CLOUD

Lalit Dashora[1], Aditya Jain[2], Gaurav Savner[3], Ashutosh Patidar[4], Virendra Singh[5]

[1]Indore Institute of Science & Technology-II, Indore (M.P.) India, dashora.lalit@yahoo.in
[2]Indore Institute of Science & Technology-II, Indore (M.P.) India, adityajain476@gmail.com
[3]Indore Institute of Science & Technology-II, Indore (M.P.) India, iamgauravsavner@gmail.com
[4]Indore Institute of Science & Technology-II, Indore (M.P.) India, patidarashu6@gmail.com
[5]Indore Institute of Science & Technology-II, Indore (M.P.) India, virendra.singh@indoreinstitute.com
Author Correspondence: 49, Ram Rahim Colony, Rau-453 331, Indore (M.P.), Mobile: +919981057041, Email: dashora.lalit@yahoo.in

Abstract: - This paper depicts cloud computing and its security issues such as multi-tenancy issue. Cloud computing is an Internet-based computing, where clients share information and resources such as servers which are provided to computers and devices. It provides people the way to share resources and services that belong to different society. Cloud Computing trend is rapidly growing that has a technology connection with Utility Computing, Grid Computing. Amazon IBM, Google's Application, Microsoft Azure etc. are examples of cloud computing. Cloud has many advantages such as flexibility, efficiency, scalability and integration. At the same time security is one of the main challenges that obstruct the progress of cloud computing. If security is not consistent, the flexibility and benefits that cloud computing has to offer will have little credibility. This paper presents a review on the various security issues of Cloud Computing.

Keywords*:* Cloud Computing, Security Issues in Cloud, SPI Model, Cloud Architecture

1. Introduction

The magnitude of Cloud Computing is mounting and have incalculably changed the way of computing in addition to it is receiving a emergent attention in the scientific and industrial communities. Essentially cloud is one infrastructure which can gratify to need of many personnel and accomplish different assortment of services. According to NIST Cloud computing can be defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Cloud computing (more concisely, but slightly less accurately), can also be defined as accessing software running on someone service providers hardware in someone else's data center while paying only for what you use [2].

Multi-tenancy and elasticity are two vital characteristics of cloud computing Model. Multi-Tenancy enables the tenants (users) to share same service instance while Elasticity on other hand enables increasing or decreasing resources allocated based on the current service demands.

2. Cloud Architecture

Cloud computing is nothing but a specialized form of grid and distributed computing which provides users a just in time infrastructure at pay per use basis. The architecture of cloud can be well defined based on three important parameters i.e. the deployment model, service model and essential characteristics.

2.1 Characteristics of cloud model

It has five crucial characteristics of cloud model, which are on demand self-service, broad network access, resource pooling, rapid elasticity, and measured device. The details are as,

- **On Demand Self Service:** On-demand self-service enables users to exploit Cloud Computing assets as required exclusive of human interaction among the user and Cloud Service Provider. In order to be effectively acceptable to the end user the self-service interface must be user friendly and afford effective means to manage the service offering.

- **Broad network access:** Broad network access fundamentally means that access is not limited to end device. It should provide access to mobile, tablet, laptop etc. For cloud computing to be an efficient substitute to in-house data centre, high bandwidth communication links must be present to connect to the cloud services.

- **Resource pooling:** The cloud must have a large and elastic resource pool to meet the clients need. Applications need resources for the implementation and resources must be allocated proficiently for finest possible performance. The resources can be physically positioned at many Geographic locations and assign as virtual components of the computation as required.

- **Rapid elasticity:** Rapid elasticity refers to the capability of the cloud that when clients need any resource it should be rapidly able to allocate those resources in addition to when the client doesn't require it should be rapidly able to withdraw those resources and reassign to other client.

- **Measured service:** The customer should be billed based on the measured usage of the cloud resources that were allocated to the particular individual. The customer should be provided the outline of resource usage in an abstracted mode.

2.2 Service models of cloud computing

The three service models of cloud computing are as,

- **Infrastructure as a service (IaaS):** Infrastructure as a service fundamentally means the service provider will provide the processing capabilities like CPU, storage, network and other vital computing resources. The consumer will not manage or control the cloud infrastructure but it will be controlled by service provider but the consumer will have the control on the operating system, deployed application, storage, and possibly limited control of selected networking components. IaaS significantly disparage the need for enormous initial investment in computing hardware such as memory, network devices and CPU time. IaaS absolutely abstracted the hardware and allowed users to utilize infrastructure as a service without bothering about the fundamental complexities.

- **Platform as a service (PaaS):** Platform as a service essentially provides an integrated set of development environment or virtual development platform accessible via web browser. Software developers can build web applications without installing the software development tools on their own computer and then distribute or deploy their apps to the cloud easily. The consumer does not manage or control the cloud infrastructure but has control over the deployed application and the environment configuration.

- **Software as a service (SaaS):** Software as a service essentially means that the service provider will provide the application hosted on providers server accessible via web browser. Everything is managed and controlled by the cloud provider. The SaaS-based applications are specifically premeditated to prop up many concurrent users (multi-tenancy) at once. Unlike the traditional method of purchasing and

installing software the software as a service customer rent the usage of the software using an operational expense model.

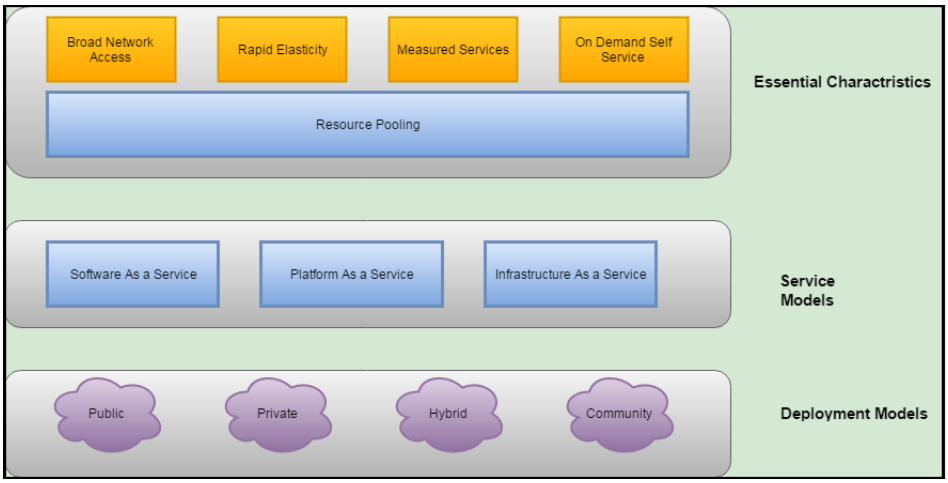

Figure 1: Visual model for cloud computing

2.3 Deployment models of cloud computing

The four cloud deployment models are,

- **Public cloud:** A public cloud is one infrastructure made accessible to universal community or business group and is owned by an organization selling cloud services. Using a public cloud can provide almost immediate cost saving to an organization. It exists on the premises of service provider. The service provider makes its infrastructure available to the universal community by means of a multi-tenant model over the Network. This is the most cost-effective model leading to extensive savings for the user.

- **Private cloud:** A private cloud is operated exclusively for a single organization. A private cloud can be managed by organization or third party. It is exclusive for an organization and nobody can share this cloud. A private cloud is also called single tenant cloud since it is privately owned by an organization. There is more control over data and resource in private cloud as compared to public cloud but the private cloud cost more than the public cloud. Also the private cloud is thought as the most secured cloud in comparison with the other cloud deployment models.

- **Community cloud:** A community cloud is only for one community not for one organization. This cloud can be for mission driven problem or for some specific community that has some shared concerns. This cloud is also managed by organization of third party.

- **Hybrid cloud:** A hybrid cloud is the compilation of two or more clouds. It can be the collection of private-community, private-public, community-public cloud.

2.4 Benefit of cloud computing

The benefits of cloud computing are as,

1. Business benefits
    - Almost zero upfront infrastructure
    - Infrastructure in nick of time
    - Most proficient resource exploitation
    - Usage based costing
    - Reduced time to market
2. Technical benefits
    - Automation and auto scaling

- Disaster recovery and business continuity
- Proactive scaling

3. Question Formalization

Now, the question comes if cloud computing is so enormous giving so many advantages, technical benefits, administrative benefits, commercial benefits then why everyone is not using cloud services. The reason here is more of fear. Firstly, the cloud acts as a hidden box (big black box) where nothing into the cloud is visible to clients. The clients have no idea or control over what happens inside the cloud. The client don't recognize whether the cloud provider is honest, even if the service provider is truthful, it can have malicious system administrative who can alter and breach privacy and integrity. Figure 2 shows some statistics about cloud computing, where several questions were asked about cloud to several companies and they were asked to grade between 1 and 5. 1 means the question is not significant and 5 means that the question is very significant. 74.6% companies said that security on a cloud is a very significant factor.

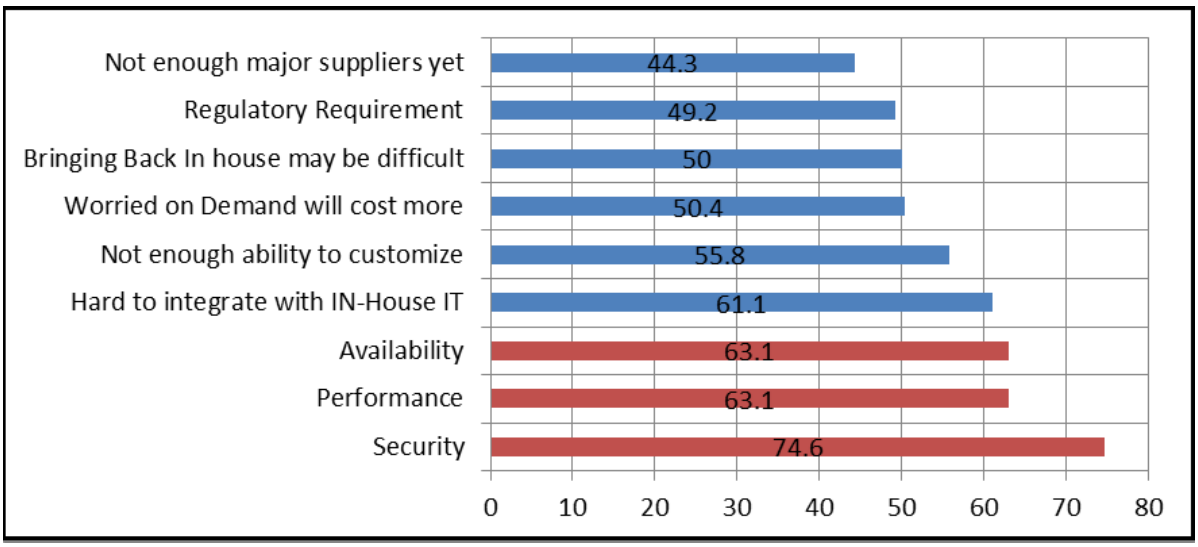

Figure 2: Survey about Certain significant questions

4. Security Issues in Cloud

To the path of success security is considered as the significant obstacle for cloud computing. Most security problems trunks from Loss of control, Lack of trust, Multi-tenancy. The client don't have the control of data, process, services (Loss of control) which is an important thing in terms of security. Other point is, can the client trust on third party (Lack of trust) who maintains all the confidential and private data. The cloud will be shared by one than one customer (Multi-tenancy) so, will the data in cloud be secured. These problems exist mainly in third party management models. In a cloud computing environment there are three sensitive states within operational context and they are:

- The emanation of confidential sensitive data to the cloud
- The emanation of data from the cloud server's to the clients computer and,
- The storage of confidential data in servers which are distant not owned by the client.

Consumers always perceive that he is losing control when he gives the data, the software, and other things to the third party. This is because all the data, application, resources are located with the provider and the provider maintains the user identity management. The consumer does not have the final control of whether the control that you have stated to the third party is maintaining it or not. The consumer relay on the provider for data security, privacy, resource availability, data security etc. The consumers don't know whether the third party can access or change the data in the consumer absence.

Trust is an additional complication which escalate security concerns to utilize cloud service since it is directly associated with the authenticity and credibility of service provider. Trust was used in the process of convincing observers that a system (model, design or implementation) was correct and secure [3]. Trust

formation might turn out key to initiate a successful cloud. Trust model is not a physical model but an ironical model on which we are somewhat relied. For defining out trust, there is no Mathematical definition. Every model shows some mathematical relations that are further used in some prospective and which becomes a measure to use any service. Trust model does not satisfy any of the mathematical relations and are described below. Let us suppose that there is a relation between two entities A and B.

- **Reflexive:** In mathematics, reflexive relation is a binary relation on a set for which every element is related to itself. 'A' may trust himself or A may not trust himself. The entity A does not trust in remembering the passwords that is why we use a system tool to show correct password.
- **Symmetric:** In symmetric A→ B then B→ A, but when we look according to trust model that A may trust B or A may not trust B. So the symmetric relation also does not satisfy the trust model.
- **Transitive:** In transitive, if A→ B and B→ C the A→ C, but this may not be the case in trust model. A may trust B but A may not trust C even if B trust C.
- **Context Independent:** In Context independent, A may trust B for something and A may not trust B for something else.
- **Temporal:** Trust is temporal; A may trust B in morning but may not trust B in evening.

So there is mathematical definition of trust but trust is ironical and is still working. So some organization may trust the service provider but the organization may not trust the third party for the same. Trust in cloud is not a technical security issue, but is the most influent soft factor.

Another Issue in cloud computing is the multi-tenant Issue. As according to the cloud computing definition the cloud is a multi-tenant model which means that the same resource can be used by certain clients over different virtual machines and that gives the client the view that the entire server is allocated to him. But this is not the case, in cloud computing the same resource is allocated to many clients as shown in figure.

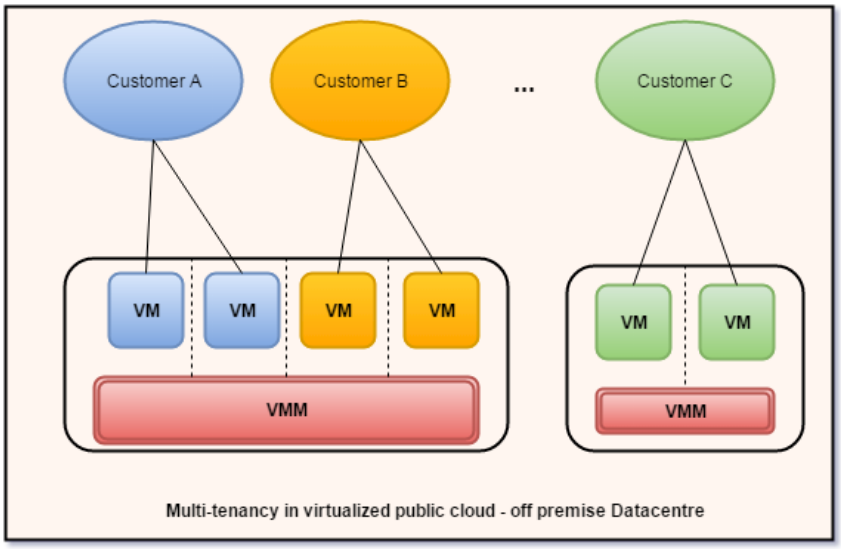

Figure 3: Multi-tenancy in cloud

The main security Issue in this multi-tenant model is that if the other user is a malicious user can affect the server by certain attacks or may try to get access to the confidential data of other tenant by attacking the cloud server by certain attacks. The malicious user may try to get the IP address of the other tenant that he is using, means malicious user may try to get the location of the storage area that the other tenant is using. The further two security issue comes under the Category of Insider Attack:

Other security issues in the cloud computing is security loopholes in software. As in software as a service (Saas) model, the client gets the service of the software on-premise. The client accesses the software and the rest system complexity is in abstraction to the client. The clients pays for the software and use the service but issue lies in that the software may have the security loopholes which the user may not know. Attackers / Hackers may identify the loopholes and may try to access the other tenant's confidential data or may try to slow down the cloud's services.

There may be certain security issues in Third party API which the client may use for authentication, authorization, auditing etc. The API of third party might have certain loopholes which in turn make a loophole for the whole cloud. The Cloud service provider provides the service to the user but may give authentication rights to the third party. If that third party API has loopholes in its own software then the whole cloud security gets breached. The further Security comes under the category of Host Level Security:

In the host level security category the first security issue is in the Iaas (Infrastructure as a service) Host security. This security issue can be understood by the figure 4. In Iaas model, the user has the control over the physical hardware in cloud. The figure 4 depicts that the user has access to the core physical hardware (physical memory, Non uniform memory unit etc.) in Iaas model but the user can have access to these hardware by using a hypervisor. In virtualization technology, there is one piece of software that allows the physical servers can have multiple instances of virtual machines and it called as Hypervisor [4]. A computer on which a hypervisor is running one or more virtual machines is defined as a host machine. Each virtual machine is called a guest machine. The virtual machines and the hardware are isolated by hypervisor. As in the figure, there are four virtual machines having different accessed to different software's and also running on different operating systems. The hardware is running four software at a time, it means that all the processes are executing in the same hardware. All these software's are running concurrently and none of them know the existence of other.

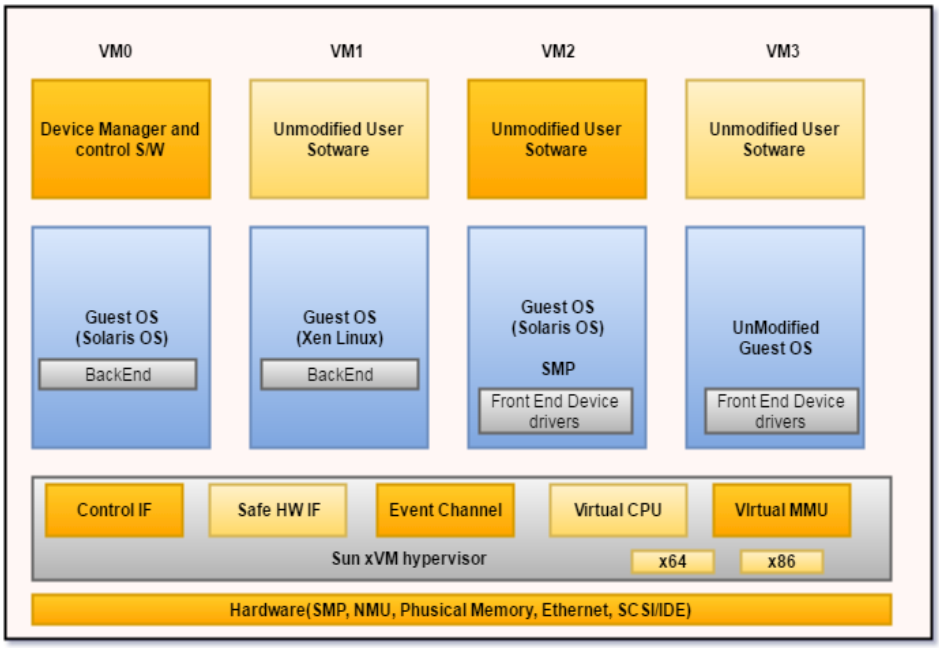

Figure 4: Detailed Iaas model

If there is a security lapse in hypervisor then everything in the cloud will have public access. So user 3 in the figure can read the data of user 2 if there is any lapse in the security issue in hypervisor because only the hypervisor is providing the isolation between the users.

If the customer is using the cloud Software as a service or the platform as a service then the cloud provider has much control. If it is Saas then there is an obsolete control, the software, operating system, the hardware and hypervisor are of service provider the user only has the control over the software. And in Paas also operating system, the hardware and hypervisor are of service provider only the software comes from outside else everything is in the control of service provider. So from the service providers point of view it is easy to provide security in Saas model and Paas model than in comparison with the Iaas model.

As the cloud computing commence could be associated with having users' confidential data stored at clients' end plus in servers, so authentication (verification) and identity management are very critical in cloud computing model. Authentication of qualified users identification and insulating such identification are part of main security issues in the cloud. Infraction in these sectors could guide to uncharted security infringement at least to some degree for some time.

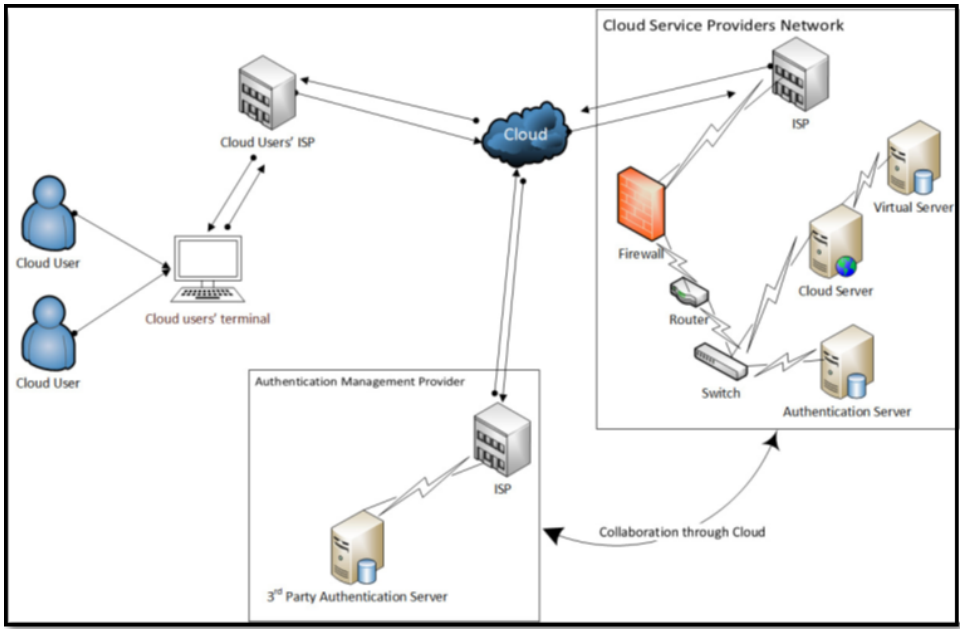

Figure 5: Authentication in cloud

The figure 5 depicts that the authentication (verification) for the purchasers will be done either by the cloud service supplier or the service supplier will contract out the identity management and authentication (verification) service to 3rd party professionals. In the subsequent case, the service provider is obligatory to have alliance with the 3rd party authentication specialist. The alliance between the service provider and the 3rd party authentication professional throughout the authentication procedure of cloud users is done essentially through cloud. This feature adds performance overheads and security issues to the cloud context as the message passing between third party authentication management authority and the cloud service provider as part of collaboration might essentially be done through cloud infrastructure [5].

The cloud computing have traditional security issues which are in other technology as well as some new security issues. Some traditional ways of security breaches are man in the middle attack, session hijacking attack, Eavesdropping, social engineering. Factors like software bugs, human errors make the security for cloud a dynamically challenging one [5].

The ultimate objective in cloud is to protect data, because data when processed becomes information and it should not be corrupted. The application manipulates the data. The application level security is protecting the data that is manipulated by the application. Between the data is born and dies the necessary confidentiality, integrity, and availability should be there. The data is first generated then it is used then further it is transferred then transformed, stored, archived and then it can be destructed. This is the life cycle of data. The data when it is generated it can be in transit i.e. it is moving from one physical location to another physical location and when this movement happens we need to ensure confidentiality and integrity using a secured protocol. This can also be done with a non-secured protocol but it requires encryption. When the data is at rest i.e. it is located in storage within a cloud needs to be stored in the encrypted form. There can certain services on the cloud like indexing, searching etc. as part of cloud. If we want to use those services of cloud on the encrypted form of data by the software provided by the cloud then homomorphism encryption is to be used. Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext [6]. The operation on the encrypted data like indexing and searching can be done after homomorphism encryption. Predicate encryption is nothing but a secret function f to which encrypted data is given as input and if the function evaluates to 1 that means that particular encrypted data item satisfies the property and if evaluates to 0 then it does not. Function f is the secret key function. When the data needs to be destructed or erased from the cloud the question arises that the data is completely erased. The data remanence is the residual data representation present even after being deleted or erased [7]. The data still remains even after we erase magnetic field and doesn't immediately get erased and remain for some time. This data remanence could lead to security breach.

5. Conclusion

Cloud Computing is reasonably a notion that confer a good number of benefits for its clients however; it also elevate some security complications which may decelerate its use. We have focused on this contrast that it is important to understand security issues which will help organizations to make the shift towards the Cloud. Since Cloud Computing grips many technologies, it also acquires their security issues. As described in this paper, Loss of control, Lack of trust, and Multi-tenancy are the biggest security concerns in Cloud Computing. Virtualization in which the same resource can be used by certain clients over different virtual machines and that gives the client the view that the entire server is allocated to him. These new concepts have certain advantages but a security issues in these can affect its success.

This paper also described about the host level security in which the Iaas host level security issues were discussed. In Iaas model, the user has the control over the physical hardware in cloud. If the customer is using the cloud Software as a service or the platform as a service then the cloud provider has much control. It is easy to provide security in Saas model and Paas model than in comparison with the Iaas model.

We have focused on other issues like the authentication issue, hypervisor issue, 3rd party API issue, data remanence issue which we consider important issues. It is important to solve such security issues for cloud success. Our research work is proceeding further to introduce a new security Issues in cloud and also aim towards providing mitigation strategies to improve its security feature.

REFERENCES

[1] Peter Mell, Tim Grance, 2009, NIST definition of cloud computing : version 15, *National Institute of Standards and Technology*, http://csrc.nist.gov/groups/SNS/cloud-computing/
[2] Lewis Cunningham, 2008, Cloud Computing Defined, http://it.toolbox.com/blogs/oracleguide/cloud-computing-defined-28433.
[3] Dimitrios Zissis, Dimitrios Lekkas, 2010, Addressing cloud computing security issues, *future generation computer systems*, 28, pp 583-592, http://www.sciencedirect.com/science/article/pii/S0167739X10002554
[4] Kamyab Khajehei, 2014, Role of virtualization in cloud computing,
[5] http://www.ijarcsms.com/docs/paper/volume2/issue4/V2I4-0029.pdf
[6] Monjur Ahmed, Mohammad Ashraf Hossain, 2014, Cloud computing and security issues in cloud, *International Journal of Network Security & Its Applications* 6 (1), pp 25-36 http://airccse.org/journal/nsa/6114nsa03.pdf
[7] Wikipedia https://en.wikipedia.org/wiki/Homomorphic_encryption
[8] J.Bhuvaneswari, R.Vaishnavi, 2013, Data Security and Storage in Cloud Computing, www.ijetae.com

A Brief Author Biography

1st Lalit Dashora – Lalit Dashora is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th year student. His research interest is computer security and database management system. He is continuing research work in security issues in cloud computing.

2nd Aditya Jain – Aditya Jain is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th year student. His research interest is in identity management in cloud computing approach can be achieved in a secured and integrated way. He is continuing research work in security issues in cloud computing.

3rd Gaurav Savner – Gaurav Savner is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th year student. His research interest is data handling in cloud. He is continuing research work in security issues in cloud computing.

4th Ashutosh Patidar – Ashutosh Patidar is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th year student. His research interest is in security aspects of cloud computing. He is continuing research work in security issues in cloud computing.

5th Virendra Singh – Virendra Singh is working as Associate Professor in Department of Computer Science and Engineering at Indore Institute of Science and Technology, Indore. He has done his thesis work (Master Degree) in the field of Genetic Programming-Network Intrusion Detection.