Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Issues in Cloud Computing: an Overview

Amina Rashid, Javed Parvez

Department of Computer Science

India

Abstract-Cloud Computing is the latest technology considered now-a-days. Cloud Computing uses the concepts of metered service i.e. pay as you go, as per the requirement of the user. Cloud Computing includes the concept of grid computing, utility in computing, and of course storage in cloud. In this paper, we present the introduction of cloud computing and emphasize on the security aspects of cloud computing.

Keywords: Data Isolation, Sanitization, Virtualization, Augmented Reality, Crowdsourcing.

I. INTRODUCTION

Cloud computing is a model, wherein pooling of available shared resources is done. It may mean data centre hosting and understood as utility computing or grid computing[1][2].Cloud computing is an extension of grid computing, distributed and parallel computing. Cloud computing is where software applications, processing power, data and artificial intelligence are accessed over Internet. There are various advantages of deploying applications in cloud which includes, low cost through shared resources, no infrastructure installation price and the most famous on demand provisioning of services.

Cloud Computing is a pool of resources where resources are collected and managed efficiently. If there are surplus resources present with the server, there is no need to purchase an additional server for computing, we can add a virtual machine to provide services for user, this concept is known as virtualization. The term virtualization has entered the field of computing and is a very important concept in cloud computing.

The cloud environment used relies on cloud providers to make decisions about data and platforms. Cloud computing provides access to data, but the challenge it is facing is to ensure that only unauthorized entities gain access. Its very critical to have appropriate mechanisms to prevent cloud providers from using customers data in a way that hasn't been agreed upon [3][4].

Various social networking sites, make use of cloud computing and are well able to handle the exchange of messages ,sharing of photos and videos over Internet, examples of which include the popular social networking sites like Facebook .Over two million businesses have adopted the Google Apps

Various security policies has to be adopted to obtain data integrity, confidentiality and data protection.

II. CLOUD COMPUTING :AN OVERVIEW

Cloud computing is the technology of the new era due to the reason that it is more flexible and accessible from anywhere and at any time. In addition, it enables sharing resources of other organizations. With the advent of cloud computing technologies, many organizations have moved their businesses to cloud, some of which include Amazons EC2,Google App Engine and Microsoft Azure, which are successfully providing services to their users.

A. Characteristics of Cloud Computing

Cloud computing is useful to separate kinds of things we have been doing online for a couple of decades from a totally new age of online software and processing power. We can very well say that the cloud is a label for online computing resources rather than the entire Internet

Cloud computing exhibits five essential characteristics defined by NIST(National Institue of Standards and Technology)[5][6].

1) On demand Self-Service: Consumer can unilaterally provision computing capabilities which include server time and network storage, as needed automatically, without requiring human interaction with each service provider.
2) Broad Network Access: Capabilities are available over network and accessed through standard mechanisms that promote user by heterogeneous thin or thick client platforms.
3) Resource pooling: Providers computing resources are pooled to serve multiple consumers using multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned accordingly to consumer demand. There is a sense of location independence in that customer generally has no control or knowledge over exact location of provided resources but many be able to specify location at higher level of abstraction.
4) Rapid elasticity: Capabilities can be rapidly and elastically provisioned in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

5) Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled and reported, providing transparency for both provider and consumer of utilized service.

Cloud computing has following types of service models:

i. Software as a Service (SaaS): customer can use the applications or services hosted on the cloud infrastructure. This is provisioning of hardware and OS, frameworks and database, for which developers write custom applications. Here, applications are accessed over Internet rather than being installed on a local computing device or in local data centre. Various SaaS applications are collaborative, allowing multiple users to share documents, their work at same time. Businesses and individuals who require direct access to cloud computing hardware on which they can run their own applications cannot use SaaS.

ii. Platform as a Service (PaaS):.Platform is software environment used to develop and run applications. Using PaaS users can obtain access to online platform provided by cloud vendor. The consumer can deploy their software and applications using the platform provided by the cloud provider. This is provisioning of hardware, OS and special purpose software made available through internet. Applications developed using PaaS can just be used by one user or few users within a particular company, but can be offered free on web

iii. Infrastructure as a Service (IaaS):IaaS provides online infrastructure on which users can store data and run or develop applications, the user needs not to manage the infrastructure but has the control over the operating system, deployed applications and storage. Hence, results in closing of data centres and local servers as data of user can be moved to the cloud easily. IaaS vendor can provide two types of servers: real or virtual.

iv. Storage as a Service (SaaS): Provisioning of database like services, billed on utility computing basis.

v. Desktop as a Service: Provisioning of desktop environment either within a browser or terminal server

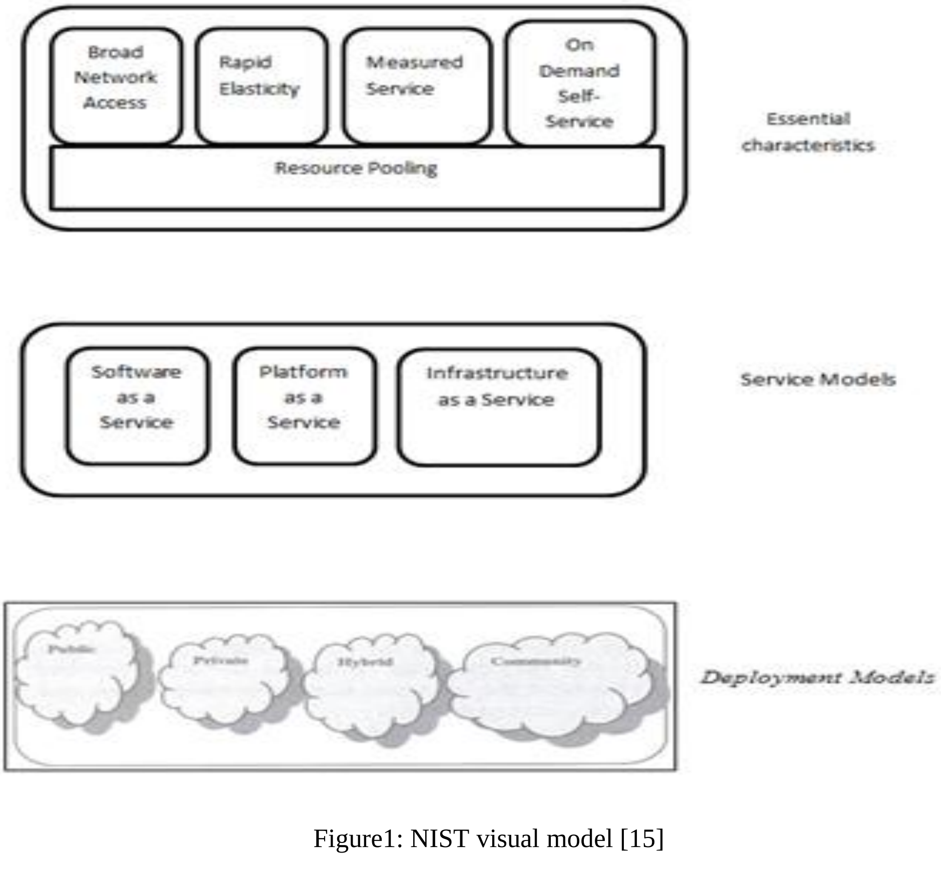

Figure1: NIST visual model [15]

Cloud computing is roughly classified into four deployment models:

1. Private: the cloud infrastructure is available for only single organization, may be managed by organization or cloud providers, on or off premise. Private cloud drives efficiency while retaining control and greater customization.
2. Public: Cloud infrastructure is made available to general public on commercial basis i.e. business rents the capability. Public clouds are for processes deemed more easily standardized and lower security risk.
3. Hybrid: combines the elements of public and private clouds.
4. Community: cloud infrastructure maintained by cloud provider or organizations and used by many organizations with similar requirements.

The major reasons for adopting cloud are as follows:

- Massive, web- scale abstracted infrastructure

- Dynamic allocation, scaling, movement of applications
- Pay per use
- No long term commitments
- OS, application architecture independent
- No hardware or software install

Cloud computing environment is a place where dynamically scalable, device independent and task centric resources are provided online, on metered basis.

Dynamically Scalable: Users only consume amount of online computing resources which they actually want at a particular point of time, which means actually selling processing power on metered basis, examples of such cloud vendors include Amazon Web Services.

Device Independent: Cloud computing is providing an environment wherein the resources can be accessed from any computer as well as any type of computer, just the prerequisite being that it should have an Internet Connection and a Web Browser.

Task Centric: The Usage model revolves around what users wants to achieve, hence shadowing particular software, hardware or network infrastructure.

B. Benefits of Cloud computing

We have entered an age which is now popularly called as cloud computing age. The cloud is based on a new kind of experience which particularly includes consumer Web space. Cloud computing is changing the way IT services were too delivered to organizations. Instead of buying and owning services, dedicated hardware and support services, IT firms are moving towards cloud computing, because it will cost them less, rather than to an in-house data centre. Various cloud vendors have also claimed that customers can reap cost saving up to 8 percent. The cloud computing from perspective of a customer is acquiring services without the need to understand underlying architecture. Cloud computing is environment friendly than the traditional computing as it removes the need of users to have high power PCs and laptops. Low power consuming computers, having processors that are composed of Intel Atoms, suffice the need of running a cloud application. Some of the marked benefits of cloud computing includes [7]:

a. Reduced Cost: The cost involved in investment of infrastructure and services are considerably reduced.
b. Flexibility: Flexibility benefits derive from rapid provisioning of new capacity and rapid relocation or migration or workloads.
c. Improved Automation: Cloud computing is based on basis that services can not only be provisioned but also de-provisioned in highly automated fashion.
d. Focus on Core Competency: The government can offer benefits of cloud computing to focus on core objectives and offer IT resources as services to citizens.
e. Sustainability: cloud computing provides the capacity to scale and manage assets more efficiently, thereby consuming less energy and resources than traditional data centres.

III. CLOUD COMPUTING ESSENTIAL FOR NEXT GENERATION COMPUTING DEVELOPMENTS

Cloud Computing is considered to being cost effective as well as energy effective, but its essentiality is equally important for next generation computing developments, such as Big Data. Hence, we can say that it will not just the desire and necessity that will drive us to do the things in effective ways, but it will also be by the demand to do the completely new things. As discussed earlier, one of the characteristic feature provided by cloud computing through SaaS is that the value is created via collaboration and data sharing. Hence, if we will not be using cloud computing ,we will not be able to obtain the benefits of new developments such as crowdsourcing. Crowdsourcing generates the value from the activities of many people using Internet, for example a problem may be worked upon by lots of people, which if would have been in the past would have been left to a single person or just a small team. Hence, lot of intellectual property is created and shared online for mutual benefit. Cloud computing will thus lead for work on various crowdsourcing projects. Developments in artificial intelligence will also depend on crowdsourced data. When it comes to next generation applications, cloud computing developments are leading to the rise of augmented reality, where real-time cloud data is overlaid on camera feed of a mobile device or a smartphone.

IV. SECURITY ISSUES

Cloud computing frees individuals and organisations from the cost and hassle of installing, maintaining and constantly upgrading software applications on their desktops and also in their data centres. It allows to focus on core competencies, rather than investing in centralized computing facilities that have to be maintained and upgraded and may not be utilized at optimum capacity. Despite various economic benefits presented by cloud computing, there are various potential risks associated with cloud service customers especially. One of the major concern, is over the security and privacy of data, because of the reason that it is stored in cloud service providers domain. The data is under control of third party, who can peep or tamper it[6].

Cloud computing creates reliance on external suppliers which also raises potential business continuity, data protection and security risks. Cloud computing makes individuals and organisations dependent on both their cloud vendors and integrity of their Internet connection. Clouds are subjected to data confidentiality, integrity, and availability and privacy issues. Cloud Computing provides data to access for only to those who are authorized users [8] and having rights to read and modify. Hence, there is requirement of authentication and identity management to protect data from unauthorized access. There are several threats for cloud computing which needs to be taken care of [5], which include following:

a) Spoofing: Accessing information by using others identity.
b) Tampering: modifying data on transit.
c) Repudiation: Denying origin of transaction (whether request or response)
d) Information disclosure: Data is disclosed to unauthorized user.
e) Denial of Service: Security intrusion that causes a system to be damaged, which is sufficient to disable atleast one of the services offered by that system
f) Elevation of Privilege: Taking privilege of accessing data without entitlement.

Data has to be efficiently secured by implementing appropriate methods to overcome threats. Data is to be protected in transit as well as at rest. Encryption of data is means to protect data at rest. There is no proper authentication of client/server. Consumers are not aware about the authenticity of intended receiver. At the same time, there are no data integrity checks, once it is received. We can generally recognize major security issues, which include identity and access management, protection of sensitive data, virtualization security and secured data migration.

1. Identity and Access Management

To control access to the information is to implement Identification and Access Management System. The system has to manage and control data based on users role, data type and users privilege to access information. IAM systems are vulnerable to some attacks like insider attacks from cloud service provider or other trusted parties.

Authentication is a process wherein credentials of user are identified. Client data is shared publically in a public cloud. Also in multitenant databases clients' data is co-mingled, there is no guarantee that data remains secure. Data that is stored is unprotected until some encryption algorithm is applied. Standards for communications protocols and public key certificates allow data transfers to be protected using cryptography.

Amazon Web Services (AWS) has removed sharing of keys and passwords [9].Amazon has provided unique security credentials to each user for accessing web services.AWS Multi-Factor Authentication (AWS MFA) is provided that offers enhanced control over AWS Account Settings and management of AWS Services and resources for which account is subscribed.

Function of Identity management is to provide necessary identifier data for authentication and authorization within business applications. The Identity Management(IDM) is regarded as the governing and operational processes that control user provisioning for information systems.

2. Protection of Sensitive Data

The sensitive data or important application when moved from organisation to cloud, where data can be readily accessed by outsider or cloud provider itself is the issue of concern. Hence, there is a need for encryption of credentials like passwords, keys, bank account details in transit over internet. Encrypting of information at cloud provider can protect against malicious cloud providers and co-tenants in cloud. Some customers encrypt their data and send the cipher text to cloud provider. Customers hold the keys so that decryption is done whenever needed. Encrypting data at rest is common within IaaS environments, using a variety of provider and third party tools. Access privileges have to be granted for data based on whether user belongs to privileged group.

Data security does not only mean to encrypt data but also enforcing appropriate policies. Data protection [11] is an important issue. Researches have implemented data protection framework [12] which provides authentication, verification and encrypted data transfer. Storage correctness, fast localization of errors and availability of data is important concept [13,14],which has to be taken care of. Challenges of Data Protection are as follows:

- Data Sanitization
- Data Isolation
- Data Location

1) *Data sanitization*

When the client data resides in the cloud, there is a vital security hurdle. Now the question that arises is that how long the data has to remain in the cloud. Till the client object refers the data, the data is available in the server. There is a chance that cloud provider might retain the information, though client is no longer accessing the data. User has to ensure that their data has to be destroyed or no longer visible in cloud provider domain, when he is migrated or terminated the service from the cloud provider. For this purpose data sanitization has to be done.

Data Sanitization is a process of making sensitive information in non-production databases safer for wider visibility. Data Sanitization also applies to backup copies made for recovery and restoration of service and also residual data remaining upon termination of service. With the proper skills and equipment, it is also possible to recover data from failed drives that are not disposed of properly by cloud providers. Data Sanitization is achieved by using masking technique [11].Masking is used to replace certain values with mask character.

The masking characters effectively remove much of the sensitive content from the record while still preserving the look and feel. Care must be taken to ensure enough data has been masked to achieve security. This is achieved by using more specific checksum algorithm. Enough care has to be taken, so that required information is not masked.

2) Data Isolation

All the data entering in the cloud provider's environment is encrypted with customer controlled keys. The data is isolated from processes and changes implemented by the cloud provider. In the database systems, isolation is a property that defines how/when the changes made by one operation become visible to other concurrent operations. In the public cloud, data has to be isolated to provide security [12].The applications deployed in the cloud include records and content related creation and usage details along with users account information.

Cloud providers need to ensure isolation of access to the software, data and services that can be protected from multiple tenants. There is a fear for security issue, which can come from lack of isolation. It is very important that cloud providers must isolate clients from each other [12].Virtualization can help for ensuring isolation within the data centre. The isolation is achieved is by running Virtual Machine instance for each user and all users can independently access data without interference. This isolation is not just a matter of securing data and applications from threats .Secure isolation is accomplished without any changes to application and operating system. Following mechanisms are used to provide secure isolation [5]:

1. Authentication: It refers to establishing/asserting the identity to the application. This is usually done in two phases. The first phase is disambiguating the identity and the second phase is validating the credential already provided to the user
2. Authorization: Authorization in broadest terms refers to enforcing the rules by which access is granted to the resources
3. Auditing: It is the process of reviewing and examining the authorization and authentication records in order to check, whether compliances with predefined security standards and policies. Also, it will aid in detecting any system breaches.

3) Data Location

One of the most common compliance issues facing an organization is data location. Use of an in-house computing centre allows an organization to structure its computing environment and know in detail where data is stored and the safeguards used to protect the data. In contrast, a characteristic of many cloud computing services is that the detailed information of the location of an organization's data is unavailable or not disclosed to the service subscriber. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. Once information crosses a national border, it is extremely difficult to guarantee protection under foreign laws and regulations. For example, the broad powers of United State of America Patriot Act have raised concern with some foreign governments that the provisions would allow the U.S. government to access private information, such as medical records, outsourced to American companies

The main compliance concerns with transborder data flows include whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post-transfer, and whether the laws at the destination present additional risks or benefits. Technical, physical and administrative safeguards, such as access controls, often apply. For example, European data protection laws [13] may impose additional obligations on the handling and processing of European data transferred to the U.S

4. Virtualization Security

Almost all Cloud providers use virtualization to provide economies of scale and optimal distributed architecture. Advantages of virtualization include multitenancy, better server utilization and data centre consolidation. Isolation of the virtual machines is one of the issue. Hypervisor can steal the data from the virtual machines. Hypervisor also called as virtual machine manager is a program to share a single hardware host by multiple operating systems. It controls the host processor and resources, takes care of allocation of resources to operating systems.

There are two types of attacks that are occurring on hypervisor [14] attack on hypervisor through the host Operating System(OS) and attack on hypervisor through a guest OS.

1. Attack on hypervisor through the host OS: Due to problems and security breaches in modern Operating System (OS) the attacks are done to gain access to host as. Since the hypervisor is simply a layer running on top of the host as, once the attacker gains control over host as, the hypervisor is essentially compromised. Hence, the administrative privileges of the hypervisor will enable the attacker to perform any malicious activities on any of the Virtual Machines (VM) hosted by the hypervisor.

2. Attacks on hypervisor through guest OS: This attack is used through guest as to gain unauthorized access to other VMs or the hypervisor. This is the most possible attack on the hypervisor, since usually an attacker can only compromise a VM remotely as the underlying host as is invisible. However, since many VMs share the same physical resources, if the attacker knows Virtualization Security in Data Centres and knowing the details VM mapping to the physical resources, he will be able to perform attacks directly on the real physical resources. By modifying his virtual memory in a way that exploits how the physical resources are mapped to each VM, the attacker can affect all the VMs, the hypervisor, and potentially other programs on that machine [14]. Figure 3 shows the relationship between the virtual resources and the physical resources, and how the attacker can attack the hypervisor and other VMs.

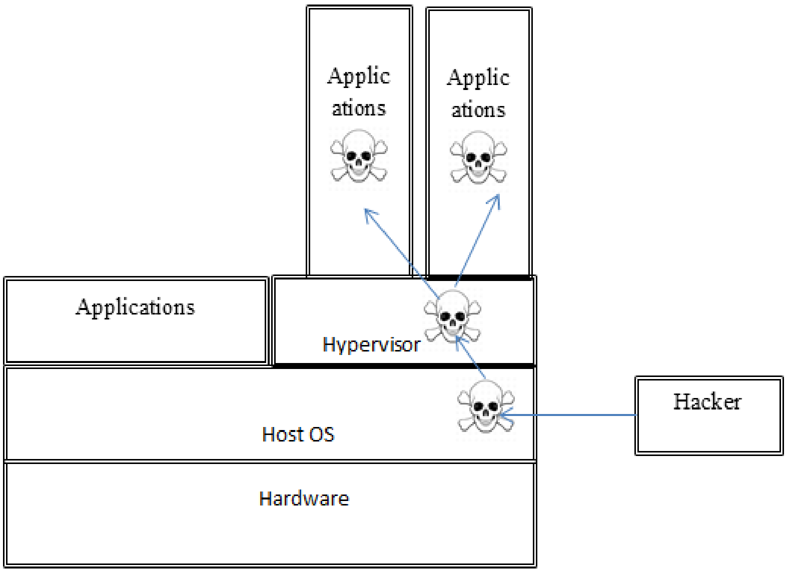

Figure2: Attack on Hypervisor through Host OS [14]

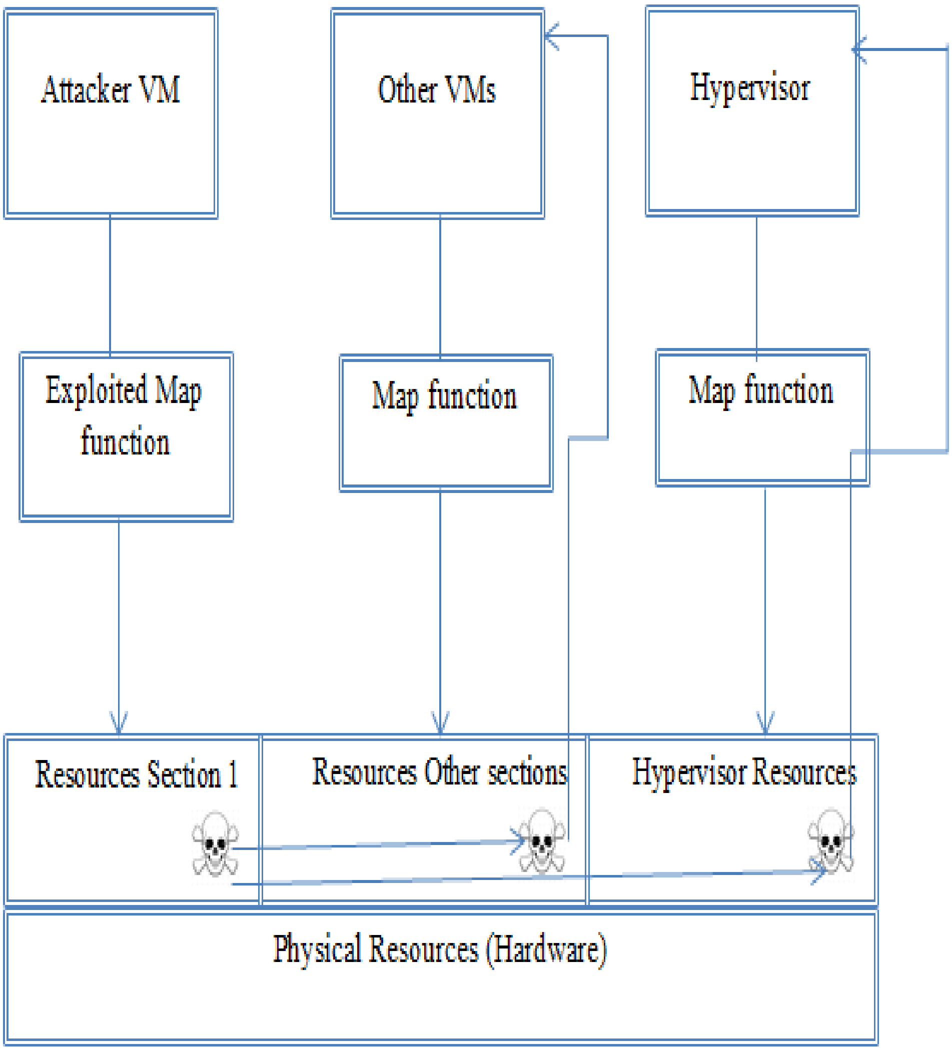

Figure 3: Attack on Hypervisor through Guest OS [14]

There other attacks other than above two attacks, which exploits the characteristics and infrastructure of virtualization. They are:

- Virtual library check-out is when a checked-out VM image becomes infected on another Virtual Machine Monitor (VMM) and later readmitted to its original virtual library. This type of attack exploits on the fact that the guest VMM may not be as secure as the original virtual library
- Migration attack is an attack on the network during VM migration from one place to another. This attack is an exploit on the mobility of virtualization
- Encryption attack is an attack used. to retrieve unauthorized information from VMs by exploiting security vulnerabilities in the virtualization software

5. *Secured Data Migration*

Data Migration is also one of the vital security issues. Data movement from one cloud to the other cloud provider due to cost or any other reasons should be completed in a secured way. If it is a cloud provider's task to migrate the data, user risk is substantially reduced. If data migration is not provided by the cloud, the consumer has to look so that data has to be either retrieved or destroyed to protect from unauthorized access. Specific provision regarding termination and process of data migration needs to be incorporated into the contract to reduce the risk of loss of data. When data has to be migrated from one cloud to another cloud interoperability becomes an important issue to be taken care.

V. **CONCLUSIONS**:

Cloud computing is levelling the playing field by bringing the potential benefits of remote and highly professional computing resources to all sizes of business. Any company or any individual can now connect to software/hardware as an online utility, with fewer companies having to invest in a large-scale computing infrastructure. In this paper, we have presented an overview of the cloud computing technique and identified various security issues of cloud computing. In this paper, we have laid emphasis on data integrity, confidentiality, and virtualization. Various security issues can be separately identified on client side and server side, with every side posing a threat to the security in the cloud computing environment. Also cloud computing services needs to take appropriate measures for ensuring safe web access, which include setting a strong password, ensuring a strong antivirus, antispyware and firewall software installed, and also ensuring that the operating system and web browser that they are using are always updated with the latest security patches.

REFERENCES-

1) Lijun Mei,W.K.Chan,T.H.Tse,"A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues",IEEE Asia-Pacific Services Computing Conference,2008
2) Thomas B Winans,John Seely Brown, "Cloud Computing, A Collection of working papers",2009.
3) Shuai Zhang,Shufen Zhang,Xuebin Chen,Xiuzhen Huo,"Cloud Computing Research and Development Trend", Second International Conference on Future Networks,2010.
4) Nuno Santosh,Krishna P.Gummadi,Rodrigo Rodrigues, "Towards Trusted Cloud Computing ",2009.
5) http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.
6) Hassan Takabi,James B.D.Joshi,Gail-Joon Ahn, "Security and privacy challenges in cloud computing", The IEEE Computer and Reliability Societies November/December 2010.
7) http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf.
8) Wayne A.Jansen."Cloud Hooks:Security and Privacy Issues in Cloud Computing". Proceedings of the 44th Hawaii International Conference on System Sciences,2011.
9) http://aws.amazon.com/iam/
10) http://www.opensecurityarchitecture.org/cms/
11) http://www.datamasker.com/datasanitization_whitepaper.pdf.
12) Fang Hao, T.V.Lakshman,Sarit Mukherjee,Haoyu Song, "Secure Cloud Computing with a Virtualized Network Infrastructure", Computer Communications Workshops,2011 IEEE Conference on 10-15 April 2011.
13)] http://ec.europa.eu/j ustice/ data -protection/index_en .html.
14) http://www.cse.wustl.edu/-jain/cse571-11/ftp/virtual/index.html
15) The NIST Definition of Cloud Computing, version 15,by Peter Mell and Tim Grance, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov) , October 7,2009