CLOUD COMPUTING: SECURITY THREATS AND TOOLS

Pallavi Marathe[1], Rashmi Chavan[2]

[1,2]Faculty of Information Technology, Shah and Anchor Kutchhi Engineering College, University of Mumbai, (India)

ABSTRACT

"Cloud Computing" is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud provides three types of services i.e. software as a service, platform as a service and infrastructure as service. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. So lack of security is the only hurdle in wide adoption of cloud computing. This report focus on the cloud computing concept, characteristics, aspects of security and most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing. The main aim of the report is to introduce some security tools available in the market.

Keywords: Bitglass, Ciphercloud , Security, Skyhigh, Skycript, Threats, Viivo

I. INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This is achieved primarily by leveraging the capacity of a data centre. Google and Amazon are two widely known data centers providing Cloud computing and storage. Software such as VMware has enabled business to create a privately owned Cloud. Along with the gains achieved in Cloud computing there are inherent security risks.[1]

While Cloud services offer flexibility, scalability and economies of scale, there have been commensurate concerns about security. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own

cloud and migrating to Cloud services. Cloud services such as Software as a service, Platform as a service or Infrastructure as a service will each have their own security concerns that need to be addressed. The report mainly focus on aspect of cloud security like CIA (confidentiality, Integrity, Availability), on basis of this security there are some security threats which also included in this report. To overcome security threats some tools are available in the market for ex. Bitglass, Skyhigh. In this report we can see different tools, their working, advantages and disadvantages and comparison of these tools and find out the best tool in the market.

II. CLOUD COMPUTING: BASIC CONCEPT

The cloud is the next stage in the evolution of the Internet. It provides the means through which everything from computing power to business processes to personal collaboration is delivered to you as a service wherever and whenever you need it. The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST):[2]

"Cloud computing is 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. This cloud model promotes availability and is composed of six essential characteristics, three service models, and four deployment models."

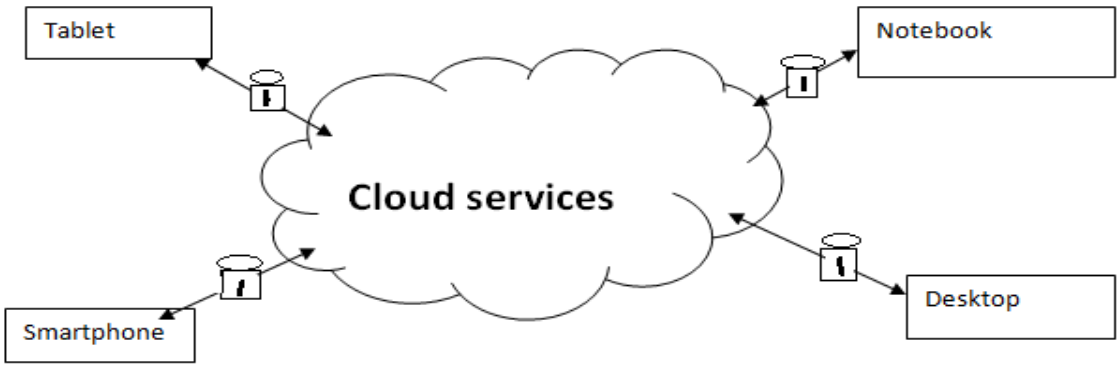

Fig.2 Example of Cloud Computing

III. SECURITY ISSUES IN CLOUD COMPUTING

There are a number of security issues related to cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. In 2013, based on a thorough analysis of Information Assurance and Security (IAS) literature, the IAS-octave was proposed as an extension of the CIA-triad. The IAS-octave includes confidentiality, integrity, availability, accountability, auditability, authenticity/trustworthiness, non-repudiation and privacy. [3][4][5]

- **Availability**

Cloud providers assure that they will have regular and predictable access to their data and applications. Data and application should available to user whenever they need it. Cloud Computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems. Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the Cloud system or applications hosted on it. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. For example, Amazon Web Services provide EC2, S3 entirely based on the virtual machine. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system.

- **Confidentiality**

Confidentiality means keeping users' data secret in the Cloud systems. Cloud Computing system offerings (e.g., applications and its infrastructures) are essentially public networks Therefore, keeping all confidential data of users' secret in the Cloud is a fundamental requirement which will attract even more users consequently. Traditionally, there are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, encrypting data before placing it in a Cloud may be even more secure than unencrypted data.

- **Privacy**

Finally, provides ensure that all critical data (credit card numbers, for example) are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

The following tips are recommended for cloud system designers, architects, developers and Testers.

1. Minimize personal information sent to and stored in the cloud.
2. Protect personal information in the cloud.
3. Maximize user control.
4. Allow user choice.
5. Specify and limit the purpose of data usage..

- **Data Integrity**

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, such as Data as a Services, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task. Furthermore, Cloud Computing system usually provides massive data procession capability. Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

- **Accountability**

Accountability implies that the capability of identifying a party, with undeniable evidence, is responsible for specific events. When dealing with cloud computing, there are multiple parties that may be involved; a cloud provider and its customers are the two basic ones, and the public clients who use applications (e.g., a web

application) outsourced by cloud customers may be another party. A fine-grained identity, however, may be employed to identify a specific machine or even the faulty or malicious program that is responsible. Accountability is a significant attribute of cloud computing because the computing paradigm increases difficulty of holding an entity responsible for some action. Following a pay-as-you-go billing model, cloud vendor provides resources rented by customers who may host their web contents opening to public clients. Even a simple action (e.g., a web request) will involve multiple parties.

- **Authenticity**

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

IV. SECURITY THREATS TO CLOUD COMPUTING

In Cloud or any security a threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire) or otherwise a circumstance, capability, action, or event. The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. There are several types of security threats to which cloud computing is vulnerable.

4.1 Threat to information privacy and confidentiality [6] [7]

- **Insecure APIs:**

Various cloud services on the Internet are exposed by application programming interfaces. Since the APIs are accessible from anywhere on the Internet, malicious attackers can use them to compromise the confidentiality and integrity of the enterprise customers. An attacker gaining a token used by a customer to access the service through service API can use the same token to manipulate the customer's data. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless.

- **Malicious Insiders:**

Employees working at cloud service provider could have complete access to the company resources. Therefore cloud service providers must have proper security measures in place to track employee actions like viewing a customer's data. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected.

- **External Attacker Threat:**

The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user

endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data.

4.2 Threat to availability

- **Sheared technology:**

The cloud service SaaS/PasS/IaaS providers use scalable infrastructure to support multiple tenants which share the underlying infrastructure. Directly on the hardware layer, there are hypervisors running multiple virtual machines, themselves running multiple applications. On the highest layer, there are various attacks on the SaaS where an attacker is able to get access to the data of another application running in the same virtual machine. The same is true for the lowest layers, where hypervisors can be exploited from virtual machines to gain access to all VMs on the same server.

- **Data Breach:**

When a virtual machine is able to access the data from another virtual machine on the same physical host, a data breach occurs – the problem is much more prevalent when the tenants of the two virtual machines are different customers. The side-channel attacks are valid attack vectors and need to be addressed in everyday situations.

- **Denial of Service:**

An attacker can issue a denial of service attack against the cloud service to render it inaccessible, therefore disrupting the service. There are a number of ways an attacker can disrupt the service in a virtualized cloud environment: by using all its CPU, RAM, disk space or network bandwidth.

4.3 Threat to data integrity

- **Data loss:**

The data stored in the cloud could be lost due to the hard drive failure. A CSP could accidentally delete the data; an attacker might modify the data, etc. Therefore, the best way to protect against data loss is by having a proper data backup, which solves the data loss problems. Data loss can have catastrophic consequences to the business, which may result in a business bankruptcy, which is why keeping the data backed-up is always the best option.

- **Account/Service Hijacking:**

It's often the case that only a password is required to access our account in the cloud and manipulate the data, which is why the usage of two-factor authentication is preferred. Nevertheless, an attacker gaining access to our account can manipulate and change the data and therefore make the data untrustworthy. An attacker having access to the cloud virtual machine hosting our business website can include a malicious code into the web page to attack users visiting our web page – this is known as the watering hole attack. An attacker can also disrupt the service by turning off the web server serving our website, rendering it inaccessible.

- **Data Segregation**

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data.

- **User access:**

Implementation of poor access control procedure secretes many threat opportunities, for example that disgruntled ex-employees of cloud provider organizations maintain remote access to administer customer cloud services, and can cause intentional damage to their data sources.

4.4 Other security threats and defence mechanism

Table 4.1 Cloud computing threats and suggested defence mechanisms for these threats

Security threats	Description	Possible defence mechanisms
Spoofing identity	The concept of spoofing identity is allowing unprivileged code to use someone else's identity, and hence, their security credentials. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.	Authentication Protect secrets Don't store secrets Message authentication codes Digital signatures Tamper-resistant protocols
Repudiation	Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations.	Digital signatures Time-stamps Audit trails
Information disclosure	Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.	Authorization Privacy-enhanced protocols Encryption Protect secrets Don't store secrets
Tampering with data	Data tampering involves the malicious modification of data. Examples include	Appropriate authorization Hashes

	unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.	MACs Digital signatures Tamper resistant protocol
Denial of Service (DoS)	Denial of service (DoS) attacks denies service to valid users. for example, by making a web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.	Authentication Authorization Filtering Throttling Quality of service (QoS)
Elevation of privilege	In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed. To exploits for other threats.	Run with least privilege

V. INVESTIGATION ON CLOUD SECURITY DLP TOOLS

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission. Adoption of DLP is being driven by insider threats and by more rigorous state privacy laws, many of which have stringent data protection or access components. In addition to being able to monitor and control endpoint activities, some DLP tools can also be used to filter data streams on the corporate network and protect data in motion. Data Loss Prevention, DLP, refers to technology employed for the purpose of reducing the risks from loss of control over sensitive data.
Some of the following tools are listed below:

- **Viivo**

PKWARE introduced Viivo in spring 2012. Viivo was developed outside of the traditional PKWARE team and methods in an effort toward "disruptive innovation" in the emerging cloud security market. Two new iterations, Viivo for Business and Viivo Pro, add administrative capabilities and support to cloud security for

large and small businesses. Viivo secures users documents before they are synchronized to Dropbox, Box, Drive and OneDrive. These servers never see copies of user data or user passphrase. Users have the keys to securing the data, not the cloud provider. Viivo uses a combination of symmetric encryption (AES-256) for the data and asymmetric encryption (RSA-2048) for the key material. Viivo uses a multi-level hybrid crypto approach when securing all of user files, whether they are personal or shared. This means that every time user gives or revokes access to a folder, it doesn't have to be re-encrypted. User files will be secure through the whole process. At the base level, Viivo creates a 2048 RSA key pair to safely exchange keys between collaborators and devices. User RSA Private key is secured with password, a secret known only to user.

Advantages of Viivo

- Compression-Files are compressed automatically before they're synced in the cloud. This cuts down on storage space and costs.
- Multi-cloud support-Data secured with Viivo can be shared and stored in all major clouds: Dropbox, Box, Google Drive and Microsoft OneDrive. Viivo also works with private clouds.
- Encrypted sharing-Lock down data with trusted encryption and seamless key management.
- FIPS compliance-FIPS 140-2 validation for encryption and decryption operations. Compliance with FIPS along NIST guidelines for Windows, Mac and iOS.

Disadvantages of Viivo

- Whtever the data uploaded by user is encrypted in the viivo folder this folder is visible to the attacker so attacker knows which tool is used for encryption.
- The file which is stored with .viivo extension, this is also visible to attacker.

➢ **SkyCrypt**

SkyCrypt, a new, FIPS 140-2 validated, military grade 256-bit AES encryption program to secure data stored on cloud storage providers and local files. SkyCrypt is the latest storage solution using the certified and proven encryption technology from DataLocker. Individuals are storing record amounts of data online with free or paid, cloud based storage providers. While these storage service providers offer great convenience, the potential for data loss or a hack of the service is high. Even so called "encrypted" providers are susceptible to unauthorized access by service provider employees. SkyCrypt solves this problem by adding a layer of military-strength encryption to cloud storage providers that is locally secured and managed by the user. With SkyCrypt, files are fully encrypted at desktop level before being uploaded and stored on cloud storage accounts. Because of the highest level of encryption, even if a cloud service provides is hacked at root level or personal logins are compromised, the files are encrypted, secure, and unreadable.

Advantages of SkyCrypt

- Transparently encrypts files on popular cloud-storage services.
- Can encrypt filenames.

- User can choose multiple layers of security including two-factor authentication. All encryption/decryption happens locally.
- DataLocker has no access to passwords.
- Can install on up to three PCs.

Disadvantages of SkyCript

- Can only share encrypted files with other SkyCrypt users.
- No Mac or mobile support.
- To share a folder, you must transmit your password and security token to the recipient.
- Sharing a single file is awkward and potentially insecure.

➢ **CipherCloud**

CipherCloud is a cloud security software suite that works by encrypting or tokenizing datadirectly at your business gateway. Unlike the previous services, CipherCloud does not aim to discover shadow IT, but to ensure the security of data contained within known clouds. CipherCloud encrypts data during the upload process, and decrypts during download. The encryption keys used for this process remain within your business network. CipherCloud also comes with built-in malware detection and data loss prevention. There are specific builds for commonly used cloud applications such as Salesforce, Office 365, Gmail and Box, as well as a variant that can be configured to work with any cloud-based applications.

Advantages of CipherCloud

For organizations, the solution contains many advanced information protection capabilities based on an open security platform.

- Enforce Data Loss Prevention.
- Deliver Malware Detection.
- Provide Activity Monitoring.
- Retain Usability and Functionality.
- Leverage Existing Infrastructure.
- Use one Gateway for All Cloud Applications.

Disadvantages of CipherCloud

- **Doesn't offer semantic security**: If the same string gets encrypted in different places, an attacker can see that the same string was used in both places. If he can figure out one of them, he automatically known the other too.

➢ **Bitglass**

Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. Bitglass is based in Silicon Valley and backed by venture capital from NEA and Norwest. Bitglass provides transparent protection for your business's data. Useable on computers and mobile devices, Bitglass aims to reduce the risk of data loss and maintain your data's visibility, even within the cloud as well as on

mobile devices.Bitglass combines a few different types of security into one package. As far as cloud applications are concerned, Bitglass is able to detect the usage of cloud applications and also encrypt data uploaded onto the cloud.Bitglass can also track your business data anywhere on the Internet, so you maintain visibility even when employees upload data onto personal file-sharing services. In addition, Bitglass protects your business against the risk of lost or stolen mobile devices. Bitglass can also wipe data on a mobile device without needing to install any agents onto the device.[8]

Advantages of bitglass

- Bitglass Cloud Discovery is available free of charge for log files up to 1 GB.
- Track down biggest potential sources of data leakage, including unmanaged BYOD, to help get a handle on where gaps exist and how to plug them.
- Bitglass Cloud Discovery is a SaaS offering requiring no software installation. Simply upload your firewall or proxy logs and the Bitglass service creates a report of cloud apps in use and their corresponding risks and categories.
- Drill down into discovered applications to learn each app's function in the business, to evaluate compliance and security across several detailed attributes, and to review the app's classification across trusted third-party security services.

Disadvantages of Bitglass

- Expensive
- Provide service to private cloud or for the big enterprise

➢ **Skyhigh**

Skyhigh Networks discovers, analyzes and secures your use of cloud applications. It uses logs from your existing firewalls, proxies and gateways to quickly discover what cloud apps your employees are using. From this, it provides you with a customizable risk assessment of all the cloud apps that are currently being used. Skyhigh's analysis tools are able to detect inconsistencies in your security policies as well as potential data leaks. Skyhigh Cloud Security Manager supports the entire cloud adoption lifecycle, providing unparalleled visibility, usage analytics, and policy enforcement. You can empower employees to use cloud services that help you grow the business while ensuring compliance with your organization's data privacy, security, and governance policies.[9]

Advantages of skyhigh

- Skyhigh's capabilities work seamlessly for the core Saleforce application as well as all AppExchange applications, Chatter, Force.com, Salesforce APIs and Salesforce mobile applications.
- Skyhigh goes beyond encryption and tokenization and provides data loss prevention, mobile-to-cloud support, application auditing, and anomaly detection capabilities across their entire Salesforce implementation.
- Skyhigh enables secure mobile-to-cloud access to Salesforce without requiring an agent on the device or VPN connection from the device, allowing customers to support their Bring Your Own Devices (BYOD) initiatives.
- Skyhigh provides these data governance capabilities while preserving all critical Salesforce end-user functionality such as sorting, formatting and searching across all fields, including custom fields.

Disadvantages of Skyhigh

- Provide service to private cloud only.
- No single user can use this service to stored data on cloud.

VI. COMPARISON OF TOOLS

Table 4.1. Comparison of Tools

Tool	Security concern	Protection mechanism	Features	Compatible Cloud
Viivo	-Privacy -Integrity -Confidentiality	-Public key cryptography -Shered folder-share key with RSA2048 -All files encryption with AES-256	-Extended customer support -Compression -Multi-Cloud support -Rights management -Mobile encryption	-Dropbox - Box -GoogleDrive -OneDrive
SkyCrypt	-Confidentiality -Integrity -Privacy	-AES 256 Bit encryption -Invisibility mechanism for folder	-Fully compatible - Free one time password utility for Android, IOS, and Blackberry devices. -Encryption made easy	-Dropbox -GoogleDrive -SkyDrive -Box -Amazon
CipherCloud	-Privacy -Data Privacy -Residency -Regulatory compliance	-Encryption- AES256 bit -Tokenization -Cloud discovery	-Encryption -Tokenization option -Enterprise key management -High performance architecture -multi-organization support	-Salesforce -Office 365 -Gmail -Box
Bitglass	-Privacy -Transparency -Mobility	-Single sign-on (SSO) -AES 256-bit encryption	-Discover ShadowIT -Detailed cloud application analysis -Ease of deployment -Control ShadowIT	-Salesforce, -GoogleApps -Office 365 -Dropbox -ServiceNow -Box -Exchange -Any App

Skyhigh	- Privacy -Regulatory policies	-Unstuctured data encryption -Selective encryption -Format preserving Encryption -Searchable encryption -Order preserving encryption	- Contextual Access Control -Application Auditing - Encryption - CloudDLP - Cloud-to-Cloud Control	-Box -ServiceNow -Office365 -Selesforce -Workday

VII. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security aspects or areas for cloud and important security threat to cloud. Also, some current solutions were listed in order to mitigate these threats. The tools mention in the report helps you to choose best security tool for protect your data on cloud. These tools are basically Data Loss Prevention tools, which help you to secure your data on cloud.

Basis on the overall analysis Bitglass and Skyhigh tool not only provide the encryption to data also discover the cloud usage. Skyhigh tool is having more advantages than other tools in this report. This tool provide encryption in many ways like unstructured data encryption, selective encryption, format preserving encryption, searchable encryption, order preserving encryption, data tokenization. By maintaining control of encryption keys, companies can ensure compliance with internal policies and external regulatory requirements including PCI DSS, GLBA, HIPAA, and the EU Data Protection Directive. Because of such encryption technique user can secure their data on cloud can get benefit from using cloud services.

REFERENCES

[1] Peter Mell, Timothy Grance ,"The NIST definition of cloud computing", NIST Special Publication 800-145,2011.

[2] David Teneyuca, "Internet cloud security: The illusion of inclusion", Information security technical report 16 (2011) 1 0 2 - 0 7.

[3] Zhifeng Xiao and Yang Xiao, "Security and privacy in cloud computing", IEEE communications surveys & tutorials, vol. 15, no. 2, second quarter 2013.

[4] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Book: Cloud Security and Privacy", 2009.

[5] Gartner Inc, "white paper: Data security in the cloud", press release, September 18, 2012

[6] K. Valli Madhavi et al, "Cloud computing: Security threats and counter measures", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[7] Vahid Ashktorab and Seyed Reza Taghizadeh **,"**Security threats and countermeasures in cloud computing" , International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Volume 1, Issue 2, October 2012.

[8] The definitive guide to cloud access security brokers for Bitglass, White paper, 2014.

[9]The 4 step Guide to cloud data security for skyhigh tool.