
Amit R. Gadekar, Dr. M. V. Sarode
PhD Scholar, SGBAU Amravati

Abstract: The word Cloud came into focus from the graphic that was often used to show the heterogeneous networks and complex infrastructure. Cloud computing is the next generation networks which is soon going to revolutionize the computing world. Security in Cloud computing is an important issue and critical parameters, and has number of issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a chance where a misbehaviors user can affect the cloud by impersonating a legitimate user, thus creating problem to the entire cloud and affects many more customers who are sharing the affected cloud. This paper works on security issues in cloud computing as well as related security concerns suggested in literature.

Keywords: Cloud computing, Security, Management, data, storage

1. Introduction:
Cloud Computing is having distributed architecture, that is centralize server resources on a platform so as to provide on demand requested computing resources and services. Its capability to save business’s extra cost by removing the need to purchase large amounts of software and/or software licenses for each employee, reducing the need for enhanced hardware, removing the need for companies to rent physical space to store databases and servers, and shifting the work load from local computers that has requested to cloud computing providers such as Google, Amazon, IBM, Microsoft, Yahoo, etc. Cloud computing is a template for convenient and any time requesting network access to a shared pool of configurable computing resources that can be quickly provisioned and released with less management efforts. In other words, Cloud Computing is the merging of a technology, platform that provides storage and hosting services on the Internet. Important goal of the cloud computing is to provide up to the mark and inexpensive on-demand computing infrastructures with better quality of service levels. Cloud computing provides infrastructure as services, platform as services, and software as services, which are made available as subscription-based services in a pay-as-you-grow model to customers. Clouds computing focus to power the next generation data centers by developing them as a network of hardware, database, user-interface, application logic services so that users should be able to access and deploy applications from any remote place where in the world on demand at competitive costs depending on users Quality of Service (QoS) requirements. Cloud service providers (CSP’s) provide cloud platforms for their consumers to use and develop their web services, much like internet service providers offer customers very high speed broadband to access the internet. Cloud service providers (CSP’s) and ISPs (Internet Service Providers) both provide services. Cloud Computing the development of distributed computing, parallel computing, grid computing, and is the merging and evolution of Virtualization, Utility computing, Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS). Infrastructure-as-a-Service (IaaS) cloud computing providers provide extra storage devices with high performance, physical, virtual computers and extra storage networking devices. It also referred as Resource Clouds likely provide resources which are managed and can easily be scaled up, as services to a variety of users. PaaS involves providing Infrastructure as a Service plus operating systems and server applications such as web servers. It supplies all the needed resources to build an application and service via the internet, without downloading or installing it. SaaS provides an application to customers either as a service on demand. SaaS is the model which hosts the application as a service to its various cloud users via internet. The user utilizes the software out of the box without any integration or patching up with any infrastructure.

2. Characteristics of cloud computing
Cloud computing exhibit five essential characteristics defined by NIST (National Institute of Standards and Technology) [1].

1. On-demand self-service. A consumer can unilaterally provision computing capabilities.
2. Broad network access. Capabilities are made available over the internet network and accessed through standard way that promotes use by heterogeneous thin or thick client platforms.
3. Resource pooling. The provider's computing resources are pooled to serve multiple customers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4. Rapid elasticity. Capabilities can be quickly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to rapidly scale in.

5. Measured service. Cloud computing systems automatically keep control and optimize resource uses by leveraging a metering capability at some level of abstraction appropriate to the type of service.

3. Security issues in Cloud:
The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where an intruder can penetrate the cloud by imposing a legitimate user, there by affecting the complete cloud. This leads to affects many consumers who are sharing the affected cloud. The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), Infrastructure as a service (IaaS). Each service has their own security issues. Following are the some security issues:

1. Data Security:
Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. The aim of availability for cloud systems is to ensure its users can use them at any place and anytime. Confidentiality means keeping users’ data secret in the cloud systems. There are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality. Integrity means not lost or modified by unauthorized users. As data are the base for providing cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task.

2. Data Locations:
When users use, they probably won't know exactly where their data will hosted and which location it will stored in.

3. Privacy:
Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human.

4. Loss of governance:
Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

5. Multi-tenancy:
Multi-tenancy referred as to sharing physical devices and virtualized resources between multiple independent users. Using this kind of arrangement means that an attacker could be on the same physical machine as the target

6. Reliability:
The cloud servers also experience downtimes and slowdowns as our local server.

7. Compliance and legal risks:
The cloud customer’s investment in achieving certification (e.g., to demonstrate compliance as per industry norms or regulatory requirements) may be lost if the cloud provider cannot provide proof of their own compliance with the relevant requirements, or does not permit audits by the cloud customer.

8. Data Recovery:
It is defined as the process of restoring data that has been lost, corrupted or accident.

9. SQL Injection attack:
Intruders inserted a infected code into a standard SQL code and it allow unauthorized person to download the entire database or interact it in other illicit ways. The unauthorized user can access the sensitive data. This will be avoided the usage of dynamically generated SQL in the code.

4. Related work:

1. Data Security:
Kuyoro et al. [2] considered that security is having a very important role in cloud computing. They cited some problems such as security of data storage on a hard disk of another person, the loss of data and the problem of piracy; if hackers use the cloud services, they would offer free or at a cheaper price to full fill their attacks. Santos et al. [4] extend the Terra [5] design that users are able to verify the integrity of VMs in the cloud. The proposed solution is called the trusted cloud computing platform (TCCP), and the whole Infrastructure as a Service (IaaS) is considered to be a complete whole system instead of granular hosts in Terra. In this approach, all nodes run a trusted virtual machine monitor to isolate and protect virtual machines. Users are given access to cloud services through the cloud manager component. The outside trusted entity (ETE) is another component that provides a trust coordinator service in order to keep track of the trusted VMs in a cluster. The ETE can be used to attest the security of the VMs [3]. To avoid access of confidential data from other users, applying encryption on that data, it makes data completely unusable and normal encryption can complicate availability. Before we need to upload data to the cloud servers the users are prompted to verify whether the data is stored on backup devices and the
keywords in files remain unchanged. Calculating the hash of the file before uploading data to cloud servers will ensure that the data is not altered [6].

2. Protection from data loss:
Data Loss can be prevented by using the Data Loss Prevention (DLP) tool which is used to track the data in motion in the cloud, detect sensitive data stored in our cloud and also data at any end point like personal computer. Enterprise Rights Management (ERM) is a mechanism which applies Digital Rights Management (DRM) to the corporate documents to control the access rights to sensitive information whether it is inside or outside of the company [8]. Tomoyoshi T. et al proposed a system to protect moving data of a company inside a USB even if it is lost. They also described the protection of document in its complete life cycle and avoiding data loss through emails [12].

3. Protection from account hijacking:
Prohibit the sharing of account credentials between employees by setting up a protocol which act as a firewall. By implementing a two-factor authentication technique the unauthorized users can be detected. A strong SLA can also be used for protect the Account Hijacking [8]. Account or service hijacking can be avoided by adopting different security features like intrusion detection systems (IDS) on cloud network. An IDS system for cloud was designed by combining system level virtualization and virtual machine monitor (responsible for managing VMs) techniques [13].

4. Multi tenancy:
To have secure multiple tenants platform, isolation among tenants data and location transparency where tenants have no knowledge or control over specific location of resources to avoid planned attacks. Always keep data at multiple location so that even if at one place attack occurs back up is in other place [19].

5. Protection from Malicious Insiders:
This type of attack can be prevented by providing different user access level control. All the login credentials are unique and limited to their own space in which they work in their data to prevent the data leakage to the malicious person [8]. The employee behaviour requirements should be made part of legal contract, and action should be taken against anyone involved in malicious activities [14]. To prevent data from malicious insiders encryption can also be implemented in storage, and public networks.

6. Authentication and Authorization:
Robust authentication and authorization helps to get effective Data Loss Prevention (DLP) solution. For every application, just user name and password is not most secure authentication mechanism. Sometime two factor or multi-factor authentication is needed [16]. In [17] the authors proposed a framework for credential classification which analyze and develop solutions for credential management that include plans to evaluate the complexity of cloud ecosystems. Tang et al. [18] proposed collaborative access control properties such as centralized facilities, agility, homogeneity, and outsourcing trust [3]. 7. Data confidentiality: This can be aware through cryptographic methods. A user check the given data block by storing the root hash of the tree; this results in a logarithmic number of cryptographic operations in the number of blocks [21]. Recent research has focused on efficiency of cryptographic methods, in particular [22] Papamanthou et.al proposes a mechanism to verify the correctness of server responses to queries, as well as integrity of stored data.

Advantages of Cloud Computing:
1. Cloud computing is more cost effective: Because companies don’t have to purchase equipment and build out and operate a data centre, they don’t have to spend significant money on hardware, facilities, utilities and other aspects of operations.
2. Always-on availability: Most cloud providers are dependable in providing their services, with many maintaining 99.99% uptime. The connection is always on and as long as workers have an Internet over network, they can get to the applications they need from practically anywhere. Some applications even work offline.
3. Improved collaboration: Cloud applications improve collaborations by allowing distributed group of people to meet virtually and easily share information in real time and via shared storage. This capability can reduce time-to-market and improve product development and customer service.
4. Manageability: Cloud computing have provided enhanced and simplified IT management and maintenance capabilities through centralize administration of resources, vendor managed infrastructure and SLA backed agreements. IT infrastructure updates and maintenance are removed, as all resources are maintained by the service provider.
5. Almost Unlimited Storage: Storing data in the cloud gives you unlimited storage capacity. Hence, you do not to worry about running insufficient space or increasing your current storage space availability.
6. Backup and Recovery: Since all our information is stored in the cloud, backing it up and restoring the same information is relatively easier than storing the data on a physical device. Furthermore, most cloud service providers are usually ability enough to handle recovery of information. Hence, this makes
the complete process of backup and recovery much simpler than other traditional methods of data storage.

Disadvantages of cloud computing:
1. Downtime As cloud service providers handle a number of clients every day, they can become overwhelmed and may even come up against technical outages. This can lead to your business processes being temporarily suspended. Additionally, if your internet connection is offline, you will not be able to access any of your applications, server or data from the cloud. 2. Security The other major issue while in the cloud is that of security issues. Before adopting cloud computing technology, you should aware that you will be surrendering all your company's confidential information to a third-party cloud service provider. This may be put your company/organization to high risk. Hence, you need to make absolutely sure that you choose the most reliable service provider, who will keep your information totally secure. 3. Vendor Lock-In although cloud service providers guarantee that the cloud will be flexible to use and integrate, switching cloud services from one to another hasn't yet completely evolved. Organizations may find it difficult to migrate their services from one vendor to another. Hosting and integrating current cloud applications on another platform may arise up interoperability and support issues. For instance, applications developed on Microsoft Development Framework (.Net) might not work properly on the Linux platform. 4. Limited Control Since the cloud infrastructure is completely owned, managed and monitored by the cloud service provider; it transfers less control over to the customer. The consumer can only have control and manage the data, information, applications, and services operated on top of that, not the backend infrastructure itself. Key administrative tasks such as server shell access, updating and firmware management may not be passed to the customer or end user.

Conclusion
Many papers were reviewed for the cloud computing, advantages and disadvantages of cloud computing, security issues in cloud computing and various techniques to solve those security issues. Each technique is aimed at solving a particular security issues. However cloud computing is still suffering in its infancy, with some positive and negative comments received on its possible implementation for a large-sized enterprise. Still many challenges and threats are yet to study. In this paper, we tried to studied security issues and their solution available in literature.

Reference:
10. Muhammad Kazim and Shao Ying Zhu “A survey on top security threats in cloud computing” in (IJACSA) International Journal