**INTRODUCTION**

CLOUD COMPUTING:

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. The cloud computing provides rich benefits to the cloud clients such as costless services, elasticity of resources, easy access through internet, etc. From small to large enterprises poignant towards cloud computing to increase their business and tie-ups with other enterprises. Even though cloud computing has enormous benefits, cloud user are unwilling to place their confidential or sensitive data, it includes personal health records, emails and government sensitive files. Suppose once data are placed in cloud datacenter; the cloud client lost their direct control over their data sources. The Cloud Service Provider(CSPs) has promise to ensures the data security over stored data of cloud clients by using methods like firewalls and virtualization. These mechanisms would not provide the complete data protection because of its vulnerabilities’ over the network and CSPs have full command on cloud applications, hardware and client’s data. Encrypting sensitive data before hosting can deserve data privacy and confidentiality against CSP.

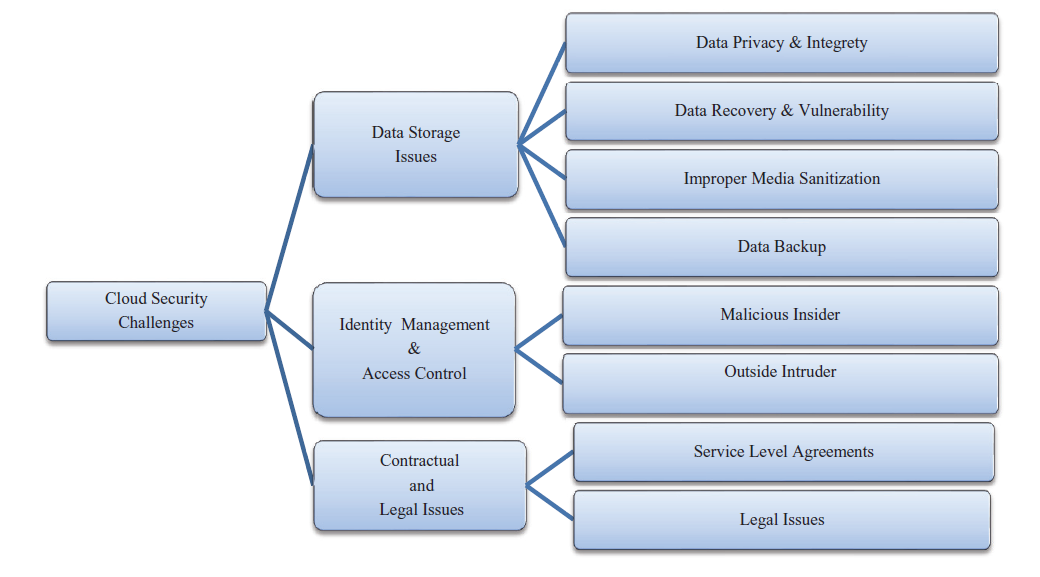


Cloud data storage model

A typical problem with encryption scheme is that it is impractical because of huge amount communication overheads over the cloud access patterns. Therefore, cloud needs secure methods to storage and management to preserve the data confidentiality and privacy. This paper mainly focuses on security vulnerabilities and issues in confidentiality and privacy over client data.

**Cloud Data Storage Challenges & Issues**

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full of control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data leads in greater security issues than the generic cloud computing model.



Cloud security Challenges

The only encryption doesn’t give full control over the stored data but it gives somewhat better than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various possibilities of attacks than in the generic cloud model.

**Cloud Storage issues**

Data privacy and Integrity

Even though cloud computing provide less cost and less resource management, it has some security threats. As we discussed earlier cloud computing has to ensure integrity, confidentiality, privacy and availability of data in generic cloud computing model but the cloud computing model is more vulnerable to security threats in terms of above conditions. Because of simplicity cloud users are increasing exponentially and applications are hosted in cloud is very high. These situations lead to greater security threats to cloud clients. If any attack is successful on data entity will leads to data breach and takes an unauthorized access to data of all cloud users. Because of this integrity violation cloud data lost multi-tenant nature. Especially SaaS providers may also lost their technical data and they have great risk over data storage. Apart from these risks, data processing also has great risk while data being transformed among multiple tenants. Because of virtualization multiple physical resources are shared among the users. This leads to launch attacks by malicious insiders of the CSP and/or organization. These situations may allow the malicious user to perform attacks on stored data of other customer while processing their data. Other major risk is when data is outsourced to third party storage by the CSP. The key generation and key management in cryptography for cloud computing is not standardized up to the mark. But without standard and secure key management for the cloud doesn’t allow the standard cryptography algorithms to perform well in generic cloud computing model. Such that cryptography may also ensures the potential risks to cloud computing.

Data recoverability and vulnerability

Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on-demand Resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users.

Data backup

The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability. In fact, the backup data should be keeping with security guidelines to prevent malicious activities such as tampering and unauthorized access.

**Identity Management and Access Control**

The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. In cloud environment, different organizations use variety of authentication authorization agenda. By using different approaches for authentication and authorization gives a compound situation over a period of time. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quickly updating and managing identity management for joining and leaving users over cloud resources. There are many issues in access control and identity management, for example weak credentials may reset easily, denial of service attack to lock the account for a period of time, Weak logging and monitoring abilities, and XML wrapping attacks on web pages.

Malicious Insiders

An insider threat can be posed by employees, contractors and /or third party business partners of an organization. In cloud environment i.e., at Cloud Service Provider (CSP) side attacks leads to loss of user’s information integrity, confidentiality, and security. This leads to information loss or breaches at both environments. This attack is precious and it is well known to most of the organization. There is variety of attack patterns performed by insiders because of sophistication about internal structure of an organization data storage structure. Most organizations ignoring this attack because it is very hard to defend and impossible to find the complete solution for this attack. This attack ensures great risk in terms of data breaches and loss confidentiality at both organization and cloud level.

Outside Intruder

Attacks that come from external origins are called outsider attacks [30]. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centers. But they must depend on the infrastructure provider to get full data security. In a virtual private cloud environment, the service provider can only specify the security setting remotely, and we don’t know exactly those are fully implemented. In this Process, the infrastructure provider must reach the following objectives:

(1) Confidentiality, for secure data transfer and access, and

(2) Audit ability.

So that outside intruders can’t access sensitive data which is stored in cloud.

ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation:

𝑦2 = 𝑥3 + 𝑎𝑥 + 𝑏

along with a distinguished point at infinity, denoted “∞”.

Elliptic curves are used as an extension to other current cryptosystems. ECC is considered as more secured algorithm than other asymmetric algorithms such as RSA and Diffie-Hellman by providing same level of security with smaller key size. For example, ECC can provide a level of security with a 256-bit public key that other techniques require a 3072-bit public key. Thus ECC has some advantages include low CPU consumption, low memory usage and greater speed. The difficulty of discrete logarithm makes ECC so important.

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products.



RSA has been developing its own version of ECC. The properties and functions of elliptic curves have been studied in mathematics for 150 years. Their use within cryptography was first proposed in 1985, (separately) by Neal Koblitz from the University of Washington, and Victor Miller at IBM. An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.