Abstract—Cloud vendors offer various services in the form of pay as you go scheme. They have become very advantageous in various fields. Some of the features are: resource pooling, storage capacity and multi-tenancy. Even though they have certain advantages, they have flaws too. The flaws are: leakage of data that is sensitive, loss of data, and so on. Cloud computing is a rising technique that provides a computing framework in the form of a service. When the users transfer their data to the cloud, they will be worried about the data security and data access control as the data is not stored inside the same trusted domain as that of the users who own this data. In order to address these issues, we may use a wide variety of key distribution and data administration techniques when the data access in demand. At the same time, the confidentiality of the data during access control, fine-grainedness and scalability must be provided. Cloud storage services are used in order to store the data on the cloud. This data is not only stored but also shared among multiple users. Security is of prime concern. Techniques like deduplication [8] and encryption to secure data on the cloud. This paper aims to highlight some of the issues encountered and the mechanisms used to combat them.

Keywords—cloud computing, shared data, access control, data leakage, security threats, malicious attacks, malevolent users.

I. INTRODUCTION

A. Cloud Computing

It is a relatively new technology that enables users to gain access to shared resources on-demand on pay-as-you-use scheme. Cloud computing provides a computing model that is used in various fields such as, in educational community and in industry. In this model, the computing infrastructure is provided as a service over the internet. They provide storage space for the users in the form of pay-as-you-go way. They help various organizations such as the governments and associations to decrease their financial overhead of data administration and store their data on a third party storage supplier instead of storing it in their data centers. This technique also enables us to access our data from any place and at any time.

B. Cloud Computing Service Models

Cloud computing is divided into three main service types:

1) Infrastructure as a Service (IaaS): They are also called Resource Clouds and provide resources that can be easily managed, as services to a variety of users. They offer virtualization capabilities. The quality of these cloud services are based on the success rate of the access of data. Infrastructure helps to equip multiple tenants at the same time as they can be dynamically scaled up or down. This service allows users to access the servers computational and storage infrastructure in a centralized service. Examples are Amazon EC2, vCloud.

2) Platform as a Service (PaaS): Applications and services are hosted on a platform which the PaaS supplies as a computational resource. It makes use of APIs to organize the performance of a server hosting engine. This completes and replicates the execution as per the request of the consumer. Examples are Microsoft Azure and Google App engine. Google App Engine allows developers to create customized apps.

3) Software as a Service (SaaS): Also known as Application Service Provider or ASP model. This model hosts several applications on the cloud as services which can be accessed via internet. The advantage of SaaS is that it is cheaper compared to actually buying an application. Examples are Gmail, Google Groups and online tax filing.

C. Cloud Computing Deployment Models

Private, community, public and hybrid cloud are the different deployment models.

1) Private Cloud: The private cloud is one which is deployed within an organization and can be used only by the members of that organization. The infrastructure is operated only for the organization that owns it.

2) Community Cloud: Shared between specific communities having similar concerns.

3) Public Cloud: Accessible by the general public or made available to large industries. Public cloud [6] is deployed in an organization in order to access various resources and web based applications.

4) Hybrid Cloud: Two or more different types of clouds that exist as unique entities but are bound together by technology.
II. CLOUD COMPUTING SECURITY CHALLENGES

Cloud implementation involves various challenging issues [4] of cloud security. Due to this reason, many companies are not able to see the advantages of cloud.

The figure is a schematic diagram showing the hierarchy of cloud computing and its security challenges on the cloud computing models. This figure includes a deployment model, service models, and issues related to networks. The deployment model consists of private, public and hybrid cloud. Service model includes the IaaS, PaaS and SaaS. The backbone for cloud computing is network.

5)Service Hijacking: The unauthorized users will gain an illegal control on certain authorized services. The various techniques are phishing and exploitation of software.

6)VM Hopping: This means that an attacker on one VM gains rights to a victim VM. The attacker will put in danger, the victim’s availability, integrity and confidentiality as he can delete the stored data and have access to victim’s resources.

B. SERVICE MODELS AND ITS SECURITY CHALLENGES:

The deployment model is classified into four categories. They are private, community, public and hybrid cloud. Security challenges includes

1)Cloning and Resource Pooling: Cloning means duplicating or replicating the data. This leads to data leakage problem which reveals the machine’s authenticity. Resource pooling is related to unauthorized access which occurs because the sharing is done through the same network.

2)Motility of Data and Data Residuals: The data is often moved to the cloud to make the best use of the resources. Because of this the enterprise is usually unaware of the location where its data is being stored. This is usually true w.r.t to public clouds. The security threats in private clouds are comparatively lesser to public clouds. The security threats may include data leakage, inconsistent data, and so on.

3)Elastic Perimeter: The private clouds usually forms an elastic perimeter. Multiple users in the organization can share the cloud resources but this can lead to data breaches. The resources are centralized. The resources are transferred based on the user’s requirements and thus may lead to problems like data loss, a user may try to access the data which is not his.

4)Shared Multi-Tenant Environment: Multi-tenancy is one of the vital attribute of cloud computing. This attribute allows multiple users to run their applications simultaneously, on the same infrastructure, by hiding their data from one and other. The issue with this attribute is that it can lead to hack attack and the resources are not distributed equally among the users.

5)Unencrypted Data: The unencrypted data can easily be accessed by unauthorized users and is easily susceptible to malicious attacks.

6)Authentication and Identity Management: This helps in authenticating the users as to who will be able to access the data stored on cloud.


A. Service Models and its Security Challenges:

1)Data Leakage and Consequent Problems: Security, integrity, data breaches occur when the data is deleted or altered without any backup. This will allow the unauthorized access of the confidential data. Deduplication is used to prevent data leakage.

2)Malicious Attacks: The attackers will have an access to the confidential data which they will retrieve and misuse. They attack the IP address and physical server. IAAS model uses virtualization as a security protection against malicious users.

3)Backup and Storage: The cloud vendor must have a backup of all the data stored on cloud. This backed up data is usually in the unencrypted form and can be easily accessed by malicious users. Deduplication is one of the solutions to reduce cloud storage and reduce backup.

4)Shared Technological Issues: A virtualization hypervisor allows access between a guest OS and the physical computing resources. The disadvantages are, these hypervisors allow the guest OS to expand to inappropriate levels of control.
But various issues that arise from identity management is that, it can lead to a problem of intrusion by the unauthorized users as well as a disadvantage of interoperability.

C. Network Issues on Cloud:
Various applications on cloud are run via internet and remote computers or servers.

1) Browser Security: Browser is used by the clients to send information on network. SSI technology is used to encrypt the user’s identity and credentials, by the browsers. The hackers will uses these credentials by making use of sniffing packages installed on the intermediary host.

2) SQL Injection Attack: A spiteful code is inserted into a model SQL code. This is a malicious attack on the cloud. This allows an unauthorized access to the database and other confidential data.

3) Flooding Attacks: The attacker will send multiple requests for the resources on cloud, rapidly, thus, the cloud is flooded with many requests.

4) XML Signature Element Wrapping: This cannot protect the position of the documents but it protects the host name and identity value from illegal user.

5) Incomplete Data Deletion: The data that is backed up in the cloud is not deleted when the original data is deleted.

III. CLOUD COMPUTING SECURITY THREATS

The top security threats [5] faced by cloud computing is as follows:

1) Data Breaches: If an attacker has access to data that is sensitive or confidential, then data breaches occur. If there is a flaw in the design of a multitenant cloud database, and an attacker gains access to it, he can manipulate every other client’s data. We use encryption as a means to avoid data breach but if we lose the encryption key all our data is also lost. This sort of information leak or disclosure is not desirable.

2) Data Loss: Data can be lost in various ways- by loss of encryption key, natural catastrophes like fire or earthquake, malicious attacks etc. This leads to denial of service. To prevent this, there must be a provision for backup.

3) Account or Service Hijacking: Phishing, fraud and exploitation of software vulnerabilities bring about what is known as service hijacking. An attacker could misuse user’s credentials for his own benefit, he can eavesdrop on activities, return false information, manipulate data and redirect to illegitimate sites. Organizations should prohibit the sharing of credentials to stop such attacks.

4) Insecure Interfaces and APIs: Customers use interfaces and APIs to interact and manage cloud services. They must be designed in such a way that the data cannot be easily tampered with.

5) Denial of Service: This is when a client is refused access to his own data or information. The attacker will send unnecessary and extra requests to the server thus sowing down the entire system.

6) Malicious Insiders: This could be an employee of the organization who has previously had authorized access to the network and attempts to misuse this privilege by violating the confidentiality and availability.

7) Abuse of Cloud Services: Services offered by the cloud could be used maliciously by attackers.

8) Insufficient Due Diligence: Cloud applications are being deployed even without proper and sufficient understanding of responsibilities such as security monitoring and encryption. In doing so, enterprises are subjecting themselves to a vast amount of risks.

9) Shared Technology Vulnerabilities: The threat of shared technology vulnerabilities exists in all three models, be it multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS). An in-depth defense strategy should include storage and computation along with user security enforcement and monitoring. A compromise on one shared technology could potentially affect the entire cloud.

10) Virtualized Technology: Making use of virtualized servers, cloud providers are able to isolate virtual machines (VM) from each other. A hypervisor is employed to manage virtualized cloud platform. Hackers are trying to attack hypervisor as that is what lies between the VMs and the underlying hardware. To avoid this, strong isolation must be implemented.

11) Unknown Risk Profile: It is important for the users to know the version of software, security practices, attempts to intrusion and updates to code.

IV. CLOUD COMPUTING SOLUTIONS/TECHNIQUES

A. Techniques Used

In the paper ‘Data Deduplication Scheme for Cloud Storage’ [3][9] the authors state that there are two strategies involved in data deduplication:

File-level deduplication: A file is a data unit and its uses the hash value as its identifier when examining the data of deduplication. When the files are compared if two or more files have the same hash value only one of the files will be stored.
**Block-level deduplication:** The file is divided into several blocks of fixed size or variable size. Hash value is computed for each block and is examined for duplication blocks.

Another paper, ‘How Data-Centric Protection Increases Security in Cloud Computing and Virtualization’ [6][10] focuses on ways to provide data-centric security. Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. Irrespective of the data being in motion or at rest it will remain protected. The possessor of the decryption keys maintains the security of that data and can decide who and what to allow the data to be accessed. Encryption procedures can be integrated into the existing workflow for cloud services. For instance the admin could encrypt all backup data before sending into the storage cloud. Corporate IP could be protected by an executive before putting it into the private cloud. A sales representative could encrypt a private customer contract before sending it to a collaborative worksite like Sharepoint in the public cloud. Public clouds house a tremendous amount of corporate data. However, there are very few security solutions that can address the cloud data security challenge that occurs when the admin, executive and sales representative use different operating systems on different computing platforms and want to share that data securely inside or outside of the private or public cloud. The security solutions for cloud and virtualized environments is data-centric file-level encryption that is portable across all computing platforms and operating systems, and works within any type of cloud.

The security of users’ data against the threats is provided by using non breakability of elliptic curve cryptography for data encryption and Diffie Hellman [7] key exchange mechanism for connection establishment. The encryption method uses the combination of linear and elliptical cryptography methods. It has three security check points namely authentication, key generation and data encryption. The technique used is KP-ABE (Key Policy Attribute-Based Encryption) [2] which is a public key cryptography method, for one to many correspondences. In this technique the encryptor associates a set of attributes to the message. Each client is assigned an access structure. There are 4 algorithms used in this scheme:

**Encryption:** This takes a public key, set of attributes and a message to output a cipher text.

**Key generation:** This takes an access tree, public key and master key as inputs and outputs a user secret key.

**Decryption:** It takes user secret key, public key and cipher text as input. Its first is to compute a key for each leaf node and it aggregate the results using the polynomial interpolation technique and then returns the message.

**File assured deletion:** When there is denial of access to the data, terminating the time of the agreement or when we totally move the data starting with one cloud first and then to the next cloud, when any of these criteria occur, the policy is repudiated and the director of the key will evacuate the public key of the associated file. Thus we can say that the file is erased.

According to Boyang Wang, Baochun Li and Hui Li, authors of ‘Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud’ [1] the first mechanism used to perform public auditing is PDP (provable data possession). This is designed to check the correctness of the data that is stored in an untrusted server. In this mechanism, we do not retrieve the entire data. In this mechanism of public auditing a cloud data, the personal user’s private data is not disclosed to the TPA during public auditing.

The problem that arises during public auditing is how to preserve the signer’s identity from TPA. If it is not preserved a particular user in the group of shared data becomes a higher valuable target to the others.

![Image of file assurance demonstration](image-url)

**[1][2] 2. Public auditing of the shared file in the cloud by the TPA.**

Let us consider that Alice and Bob are in the same team and they share a file on the cloud. The file is divided into many blocks and is signed independently by the users. If the block in this shared file is modified by the user, this user must sign the modified block. Using their private/public key pair. The signer’s identity on each block must be known to the TPA so that it can audit the integrity of the whole file based on requests from Alice or Bob. From the figure, after performing several auditing tasks, the private/sensitive information is revealed to the TPA. If most of the blocks in the shared file are signed by Alice, it indicates that she has an important role in the group.
The 8th block is frequently modified by different users, which means that there is a valuable data that needs to be discussed among Alice and Bob and change it several times. The drawback of this technique is that, the identities of the users on each block will reveal confidential information that must be kept only among the group members, to the TPA. Thus, public auditing on the shared data cannot be performed while still preserving the identity privacy.

In this paper [1] the proposed mechanism is called Oruta. It is a new privacy-preserving public auditing mechanism for the shared data stored in an untrusted cloud. The technique used in this is, we use ring signatures to construct homomorphic authenticators so that the TPA is able to verify the integrity of the shared data without retrieving the entire data, for a group of users, while the signer’s identity on each block in shared data is kept private from TPA. Homomorphic authenticator is a basic tool that is used to construct data auditing mechanisms.

This mechanism also supports batch auditing which means that multiple shared data can be audited simultaneously in a single auditing task. This mechanism makes use of random masking which is used to support data privacy during public auditing and it also uses index hash tables to support dynamic operation on shared data.

To combat the threats posed by cloud security, TrendMicro has come up with a new technology called SecureCloud [16]. It makes use of patented key-management techniques and encryption to control cloud data access.

**Easy deployment:** The agent is installed at the virtual machine. Data is rendered tamper-proof due to the encryption at kernel level. Man-in-the-middle attacks are thus eliminated.

**Secure key management:** Cloud consumers have their own encryption keys therefore they control their own data. It is not managed by cloud service provider, but rather by TrendMicro or the consumers themselves.

SecureCloud uses VM-level encryption, which uses different keys for different consumer information.

**Industry standard encryption:** SecureCloud uses AES encryption and those who have on access to the encryption key cannot read or use the data. This reduces risks of data theft, unauthorized access or data seizure. Encrypted data is very secure.

**Granular control:** We can determine which server gets access to secure data. SecureCloud also offers specific permission levels to system administrators.

**Custody encryption keys:** SecureCloud keeps all encryption keys isolated from the cloud infrastructure provider. In case of data theft, the encrypted data becomes useless due to lack of encryption keys.

**Reporting:** SecureCloud provides detailed logging and reporting of all actions performed.

All events are logged and can be viewed when required.

**B. Recommended Practices**

As per the McAfee blog, the top 15 practices [20] suggested for cloud users are as follows:

1. Cloud services must be managed and security must be maintained using monitoring, security tools and services.
2. Before entering into a contract with the cloud provider, ensure that internal security is up to date.
3. Choose what goes on the cloud and what does not. Precautions and tools to be used must be explicitly stated.
4. List down services that are deemed by the IT as acceptable and secure.
5. Start cloud use with low-risk functions.
6. Testing software using sensitive customer information should be forbidden.
7. Read through the Service Level Agreement (SLA) carefully. Ensure there are no loopholes.
8. Negotiate with the cloud service providers as per your needs and requirements. Use hybrid model for scalability and cost benefits.
9. The data providers’ strategies must be examined if relevant.
10. Look for standard certifications of the providers. If there are any security gaps, fill them. If a third party is involved, check their audits as well.
11. You must be allowed to periodically audit your security.
12. Always look for services that comply with industry standards.
13. Data must be encrypted before it goes on the cloud.
15. Most often users access cloud via web browsers. Make sure the web browsers are free from malicious use and browser exploits.
V. CONCLUSION

Cloud computing is dynamic, known for its flexibility, multi-tenancy and high capacity storage. But it is subjected to vulnerabilities and threats. The need of the hour is to build in-depth and top-technologies used to combat security issues faced by the cloud. In this paper we have studied some of the technologies used to secure cloud.

Acknowledgement

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES