Authentication key generator for data sharing on cloud| A Review

Esikala Nithish Mani Krishna

Gangireddy Ramyasri

Gundre Sai Sruthi

NEW HORIZON COLLEGE OF ENGINEERING

Abstract:

Cloud computing provides services through the Internet on demand with the help of a substantial amount of virtual storage. The main advantage of cloud computing is that it eliminates the need for customers to install expensive computing infrastructure. Infrastructure and its associated costs are lower. Recent developments in cloud computing and other industries have prompted researchers to explore new, pertinent technologies. Both individual users and businesses upload their software, information, and services to the cloud storage server because of its accessibility and scalability for computer operations. No matter what While moving from local to remote computing has its benefits, several security concerns and challenges for the provider and the client. There are numerous cloud services available from dependable third parties, increasing security issues. The cloud service provider offers its services over the Internet and makes use of numerous online technologies, which raises fresh security concerns. One of the most important requirements today for every firm is online data exchange for greater productivity and efficiency. For this we are generating the multiple key to give access for user, admin and many other people related to the work to retrieve the data. By this data owners can save and share the data through online.

1.Introduction:

With the recent emergence of cloud computing, countless applications that span international boundaries and include millions of users have seen their ability to share data stretched to the limit. Today, governments and businesses view data sharing as a crucial instrument for increased efficiency. Social networking, healthcare, and education have all been transformed by cloud computing. The capacity of cloud computing to enable global data sharing and exchange between numerous users without the pains of manual data transfers and without the production of redundant or outdated documents may be its most intriguing use case. Social networking sites have made the globe more interconnected by utilising the cloud to enable the sharing of text and multimedia. Cloud platforms frequently feature collaborative tools, which are very well-liked since they increase productivity and effort synchronisation. The impact of cloud computing has spread to the healthcare industry as well,

with smartphone applications enabling remote patient monitoring and even diagnosis. In summary, cloud computing is drastically altering many facets of our existence. Despite all of its benefits, the cloud is vulnerable to security and privacy breaches, which pose a serious obstacle to its widespread adoption as the main method of data sharing in today's society. In a poll conducted by [1] cloud customers ranked security as their top difficulty, with 75% of users concerned about the security of their vital IT and business systems. Malicious service providers must also be considered, notwithstanding the prevalence of security risks from outside agents. It is not simple to guarantee security and privacy on the cloud because online data almost always resides in shared environments (for example, many virtual computers running on the same physical device). Setting down the specifications that a data sharing service must meet in order to be considered secure is crucial when discussing the protection of data privacy and security in the cloud.

2.The architectural framework for cloud computing:

The fundamental architectural framework for cloud computing is provided . The fundamental idea and architecture of cloud computing must first be understood in order to comprehend the security concerns. The widely used NIST provides four deployment models, five basic characteristics, and three service delivery models [2].

2.1. Fundamental qualities

There are many attributes of cloud computing, but in this article we concentrate on five key attributes listed by [2]:

2.1.1. On -demand self-service

It allows customers to use web services and administration interfaces to direct request, manages, and access services without interacting with any human beings.

2.1.2. Access to a large network

Any standard device, including smartphones, PCs, desktop computers, and laptops, must be able to accesses data and services that provided in cloud. These devices operate using some common technology and protocols. Because of its nature, cloud computing ought to accommodate all established protocols.

2.1.3. Resource pooling

Large physical or virtual computer resources are made available by the cloud provider and are distributed among numerous consumers. In a multi-tenant setting, these resources are assigned in a dynamic manner.

2.1.4. Rapid elasticity

One crucial characteristic of the cloud is elasticity. The resources used for this property are scaled based on consumer needs. Customers have infinite resources that they can pay for on a pay-per-use basis as needed.

2.1.5. Measured service

The cloud system's metering functionality allows the resources to be automatically controlled and scaled in accordance with user demand and paid services.

2.2.Service paradigms

A set of services is supplied by the service model; the consumer uses these services, which are offered by the service provider.

2.2.1.SAAS

In order to reach the applications and move the data and applications to distant storage servers using online software services, the SaaS offers its clients (IDE). Customer relationship management (CRM) and Salesforce.com are two examples that fit the SaaS paradigm.

2.2.2 IAAS

The phrase "IaaS" refers to the virtualized resources that the cloud service provider makes ad-hoc and on-demand available, including computing, storage, network, memory, and processor. Amazon Web Service [3], which provides EC2 services like virtual machines with a software stack, is the best IaaS example.

2.2.3 PAAS

The platform-oriented cloud provides Platform as a Service, a more complex programmable platform. To build, execute, deploy, and manage their applications, cloud users can make use of a range of programming models, an IDE, specialised services, operating systems, and platform-level resources on an easily programmable cloud platform.

2.3. Deployment models

The various cloud types are described in the cloud computing deployment model.

2.3.1 Private cloud

An exclusive cloud is internally controlled and operated by a single business or a third-party auditing service (TPA).

2.3.2 Public cloud

The CSP operates and manages a public cloud, and the user's off-site location may host the actual infrastructure. The resources in the cloud are shared by many users, who pay the cloud provider for the services they utilise.

2.3.3.Hybrid cloud

Two or more clouds with the same architecture and capabilities can be combined to create a hybrid cloud.

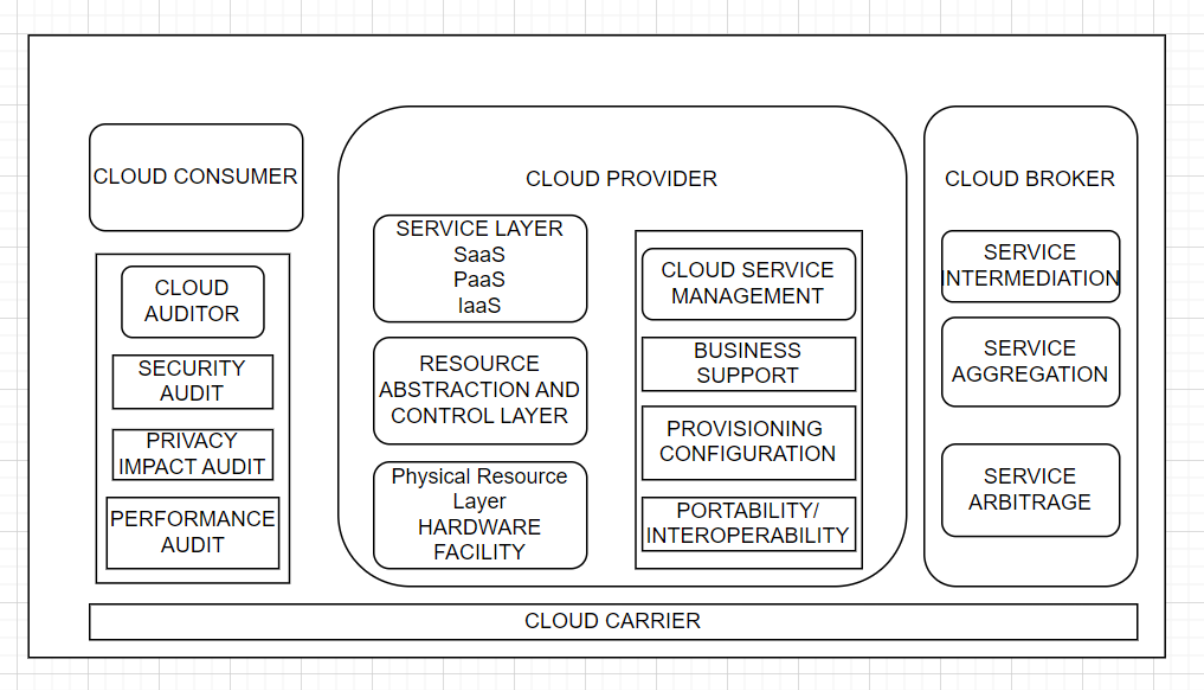

Fig 1 : The architectural framework for cloud computing

3.Methods of cloud security issues:

3.1.Data storage:

Loss of control in the data storage problem is a serious issue since the cloud computing model does not allow full control over the data and makes it more challenging to verify data integrity and secrecy. The cloud computing consumer is geographically disconnected from their server for data and storage of computing. The use of cloud computing offers a pool of servers used to store cloud data. The server pool's location is Unknown, and the cloud service provider is in charge of and manages it. Finding the actual layer is more difficult due to the virtual layer's abstraction.

Data pooling, data locality several locations, remote data storage, loss of control, and sophisticated models for integrity verifying the solution are some examples of security challenges with data storage.

3.2.Untrusted computing:

The front end interface for SaaS applications is often what security services want to provide when users request a web service or an HTML page. These programmes can be modified or adjusted to fit a certain pattern of behaviour. The session state manager, extra services, and any possible reference data that the request may call make up this pattern of behaviour. The request is simply forwarded from one service to another, and so on, building a service tree whenever one application or service calls another. A computing framework that computes massive data sets in distributed systems may result in the undesired, unreliable, and dishonest outcome as a result of server misconfiguration and malicious activity.

Security issues with untrusted computing are Top-down SLAs. Dishonest computing, malicious users, outages, slowness, and others[5,] Inadequate computer model security measures, root-level backup errors[10], migration and restoration challenges, sluggishness and outages Data and service accessibility utilising phoney resources[11].

3.3.Service and data availability:

The real and virtual resources of the cloud's database and processing servers are extremely accessible. To achieve high availability and scalability of services and data, architectural changes must be made at the application and infrastructure levels. One approach is to run apps on several servers. The use of this tactic enables DoS attacks. The benefit of this approach is the availability of a backup application server in case the primary one fails, guaranteeing the availability of data and services. The server could also be working on a particularly demanding application job, in which case he will consume more power, resources, and time. The cost of further calculations and application availability are probably increasing as a result Counterfeit resource utilisation and Cloud disruption are security concerns with data and service availability[12,13,14].

3.4.Cryptography:

Information and data stored in the cloud are protected using cryptographic techniques. The concept behind achieving cloud security is simple. It transforms plain text matter into cypher text, variety type of text. The concept is predicated on the notion that, in the event that a cypher text is available, it is impossible to calculate the value of the plain text data. Since the entire security depends on the key that is used as an encryption key, they need to design cryptography techniques carefully and strongly. The Rivest Shamir Adleman (RSA)-based encryption is more secure thanks to the prime factorization of large numbers.

Hardware availability is one of cryptography's security concerns (hardware fault) Ineffective key management[15], flawed cryptography algorithms, brute force, and dictionary attacks are all examples of insecure cryptography mechanisms.[17]

3.5.Data recycling:

Reusing the cloud space after the data had been effectively used and disposed of was a smart idea. But the next user must be prevented from accessing the data that was used by the preceding user. Sanitization is the process of clearing out or eliminating specific pieces of data from a resource. People can access updated data in a dispersed manner following sanitization. To correctly dispose of data and choose the data that is delivered to the garbage, data sanitization is a crucial task in distributed systems. Because the hard drive can be erasing some crucial data, incorrect sanitization leads to data leakage and loss.

The ineffective application of data destruction policies[18], the disposal of unused hard drives[14], the use of hard discs by many tenants[15], and resource recycling[19,20,15] are security concerns with cloud data recycling.

3.6.Malware:

It is active and performs activities at every three minutes at a single business. An online data storage system is MediaFire and SugarSync cloud-based service provider generates a distinct security issue they either copy the features and data properties of the many devices. The primary issue there is that if one system contains then, because of inheritance, the malware spreads throughout the cloud. Malware also poses a serious threat to cloud devices because it can be used to corrupt or erase cloud data. The security issues of malware are failure of signature based anti viruses, cloud malware syncing [21].

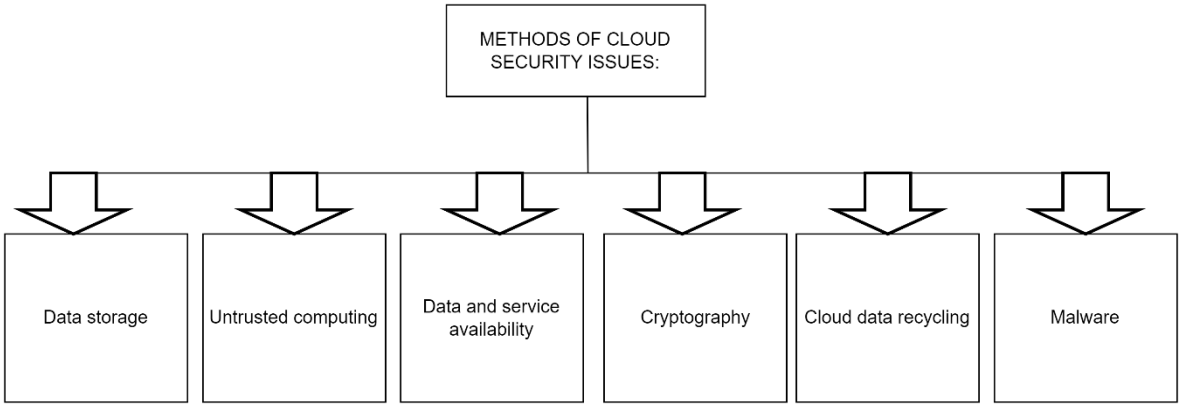

Fig 2 : Methods of cloud security issues

4.Cloud protection

Computer security includes cloud security. It specifies a system of regulations, controls, and technologies that are useful for safeguarding data and services. Threats and attacks have an effect on the cloud system either directly or indirectly. New security issues might arise as a result of the cloud resources' integrity, availability, and confidentiality being compromised, as well as the services offered at different levels. In this part, we'll look at a few security concepts in order to have a better knowledge of cloud security issues.

4.1. Concepts for cloud security

Cloud security addresses a variety of security issues and threats. The report highlights the origins of the vulnerability and threats to help readers understand the concept of cloud security. This section discusses certain cloud-specific issues, such as virtualization, multi-tenancy, cloud platforms, data outsourcing, data storage standardisation, and trust management, to better understand the security issues that are common in the cloud.

4.1.1. Aspect in virtualization

Virtualization is the concept separation of services, programmes, computing resources, and operating systems from the physical hardware on which they are run. A component of virtualization is the virtual machine (VM) and virtual machine manager (VMM).

4.1.2. Multi-tenancy

A characteristic of the computing environment called multi-tenancy introduces the idea of sharing, allowing one or more tenants to share each running instance. It offers the option for multiple users to share a single cloud platform. Think of an IaaS provider. A multi-tenancy sharing platform is referred to as a VMM, and instances are referred to as VMs.

4.1.3.Threat agents

Threat agents are a type of entity that can fend off an attack and create threats. Whether it occurs internally or externally, this threat is caused by a person or any software programme. A network level attack is sent by an external software programme or external person known as an anonymous attacker via a public network. Those who live in the cloud environment without the administrator's authorization are considered untrusted cloud service users.

5.Threats to cloud computing:

Anything that has the potential to seriously harm a computer system is considered a threat in the context of computer security. Potential attacks on the computer system or network infrastructure may result from threats. The biggest risks to the security architecture of cloud services were described in the study by [22]

5.1.Different service delivery :

Both the business model and the cloud computing model use unique methods for delivering and receiving services. Therefore, cloud computing has the flexibility to alter its own method of service delivery. The firm must evaluate all the risks associated with losing control of the cloud because the cloud service provider has transferred all services and applications to a remote location. When sending cloud data between two locations, security rules specific to each location must be followed. This is one of the key risks that are brought about by using

something. To eliminate such threats, one needs robust end-to-end encryption, globally recognised security regulations, and a trust application.

5.2.Misuse and criminal application of cloud computing:

Information as a service suppliers offer these utilities, including limitless network, storage, and bandwidth. Some service providers permit users to utilise their products for a predetermined trial period. This is frequently paired with a hassle-free registration method that allows anyone to register without going through a secure procedure and access cloud services. Currently, they don't have enough power to affect the user throughout the trial period. The hosting of hazardous material, password and key cracking, captcha solving farms, and distributed denial of service (DDoS) attacks are further possible threats. As a result, spammers, programmers of malicious code, and other criminals can execute their attack. These flaws put the platform-as-a-service and information as a service infrastructure at danger.

5.3.Unsecured software interfaces and APIs:

To interact with cloud services, customers can use a variety of software interfaces and APIs provided by the cloud provider. The layer-like placement of these interfaces on top of the cloud foundation adds to the cloud's complexity. These interfaces offer their customers full provisioning, management, and monitoring capabilities. As a result, the security of these APIs is crucial to the cloud's availability and security. But occasionally, both deliberate and unintentional attempts can compromised the security to these APIs. PaaS, IaaS, and SaaS service models may be impacted by these kinds of API attacks.As other parties frequently use these interfaces to deliver services, there is also the possibility of another form of risk.

5.4.Malicious insiders:

Malicious software one of the main dangers of cloud computing. internal dangers, as a result of many organisations' lack of details regarding her access level and employee hiring process for their workers of internal resources. Mostly, this threat is carried out.because of the clients' use of IT services, lack of transparency, and collaborating inside a single management domain. Somehow, a worker a greater amount of access as a result, the confidentiality of Services and data are compromised. This also leads to a circumstance in which an insider attacker could acquire sensitive information and impact the cloud.

5.5.Issues with shared technology in a multi-tenancy setting:

Information as a service providers leverage the virtualization idea to deliver the services in a multi-tenant environment. The ability to share the same resource among several users is made possible through virtualization. In a multi-tenant system, the hypervisor could give information about the user to a rogue user. This is a serious risk because the infrastructure is not built to provide effective isolation in a multitenant setting. By allowing one user to access information about another user, sharing could have an impact on the cloud architecture as a whole. Strong authentication and access control are two methods for avoiding this issue.

5.6.Data leakage and loss

The collaborative and productive nature of computing in cloud, data loss can also result from the loss of an encoding key. Theft, modification, and deletion of data without a backup of the original data are a few examples of data loss. Weak encryption techniques, weak keys, association risk, unstable data centres, and a lack of disaster recovery are the main causes of data loss and leakage. Weak access control, authorization, and authentication are other contributing causes. All service model types are vulnerable to these dangers. Safe APIs, data backups, powerful encryption keys, secure storage, and data integrity are a few prevention strategies.

5.7.Hijack service:

The customer may be forcibly steered to a risky website during the service hijacking process. Fraud, phishing, and the usage of software bugs are all methods that can be used to accomplish this. Reusing login credentials and passwords frequently results in these attacks. In cloud computing, if a hacker gets hold of someone's login information, they can record actions, modify data, return fake information, or divert the client to compromised accounts and unapproved websites.

5.8.Risk profiling:

Cloud services are less involved in owning and maintaining infrastructure and software because of the high workload. The cloud offers contracts to businesses for the upkeep of their software and infrastructure. The cloud does not comprehend the organization's internal security procedure, patching [23], auditing, security regulations, hardening, or logging process, despite the fact that this theory is sound. This ignorance leads to greater threats and dangers. The cloud should have a mechanism in place for keeping an eye on and making changes to logs, data, and infrastructure-related information in order to eliminate threats.

5.9.Identity theft:

Identity theft is a type of fraud in which a perpetrator uses another person's name, credentials, resources, or other service benefits in order to get access to protected information. The victim suffers several unpleasant consequences and financial loss as a result of these threats. Keyloggers, phishing scams, and inefficient password recovery techniques, among other things, may all contribute to this danger. The security idea includes both strong multi-tier authentication techniques and a trustworthy password recovery procedure.

THREATS

Threats	Effects	Solutions
Different service delivery	Loss of control over the infrastructure of the cloud	provided services that were controlled and supervised
Misuse and criminal application of cloud computing	Due to unclear sign-ups, there is a loss of validation, service fraud, and a stronger attack.	Observe the state of the network and use strong registration, authentication methods.
Unsecured software interfaces and APIs:	Incorrect transfer of the content, improper, authentication, and authorization	Strong access control and authentication measures are used, and data transfer is secured.
Malicious insiders	resource penetration, asset damage, productivity loss, and operational impact	Utilization reporting and breach alerts, as well as open security and management procedures
Issues with shared technology in a multi-tenancy setting:	By exploiting the hypervisor, interfere with one user service and other user services.	Audit configuration and vulnerabilities, and utilise strong authentication and access control procedures for administrative tasks.
Data leakage and loss	Data that is personally sensitive may be altered, destroyed, damaged, or erased.	provide systems for data backup and storage
Service hijacking	Stolen user account credentials give access to a crucial region of the cloud, putting the security of the services at risk.	use of powerful authentication techniques, security guidelines, and encrypted communication
Risk profiling	Operations involving internal security, security guidelines, configuration breaches, patching, auditing, and logging	Recognize incomplete logs, infrastructure, and data aspects in order to safeguard the data use monitoring and altering system.
Identity theft	To access that user's resources and obtain credits or other benefits under that user name, an aggressor can obtain the identity of a legitimate user.	Authentication methods and strong multi-tier passwords should be used.

Table 1: Different types of threats, their effects and solutions

ATTACKS:

Attacks	Effects	Solutions
Zombie attack	Affected service availability; possibility of creating a phoney service	robust authorisation and authentication
attack using service injection	Service integrity is compromised, and users are given malicious services in place of legitimate services.	Service integrity is compromised, and users are given malicious services in place of legitimate services.
port checking	Unusual service behaviour reduces service availability	Strong port security is necessary
Phishing attack	Affect the user's private information that shouldn't be shared	employ a secure web link (HTTPS)
attack through the backdoor	has an impact on the service's accessibility and data privacy, and offers rights for accessing legitimate user resources.	Strong authentication, identification, and isolation procedures are necessary.

Table 2: Different types of attacks, their effects and solutions

Conclusion:

Cloud computing include rapid system implementation, low costs, abundant storage, and simple system access from anywhere at any time As a result, cloud computing is becoming more and more apparent in recent technical developments and a widely utilised computer environment everywhere. Several security and privacy issues make it difficult to use cloud computing. The security weaknesses, dangers, and assaults that the cloud already has should be known to all users. If businesses are aware of security threats and attacks, they can adopt the cloud more swiftly.. Utilizing both traditional and cutting-edge techniques and technology, cloud computing. Multiple clouds can be produced using this innovative technique. Particular security concerns. The ability to access the same physical resources from the cloud from several places thanks to virtualization and multi-tenancy features. The security of the system may be hampered by improperly segregated VMs. We can increase cloud security and lessen risks and assaults by creating the keys.