International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

Review on Security Concerns in Cloud and an Overview of Cryptographic Algorithms to avoid Security Issues

Anusha.Srinivasa

Department of Computer Science Engineering
JSS Academy of Technical Education

Abstract - In today's world, Cloud Computing is all over the place. Furthermore, it very well may be characterized as an enormous stockroom of information stockpiling. Cloud computing empowers undertakings to be allocated to a mix of programming and administrations over a web. Cloud administration merchants have the information of the information proprietors in their workers and the clients can get to their information through these workers through a Web supports. Consequently, Cloud empowers the association to arrangement an expense productive and viable framework practically and it follows pay as you use premise. The issue here is as the data owners and the servers are two different individuals, hence proper care has to be taken so that data is stored in a secured manner with proper encryption.

1.INTRODUCTION

Cloud computing can be characterized as the "conveyance of processing administrations (workers, stockpiling, data sets, organizing, programming, examination, insight and that's just the beginning) over the Internet". Here we normally pay just for cloud administrations we use; it helps in bringing down our working expenses and assists us with running our framework all the more productively.

2. Types of cloud:

There are three ways to set up a cloud service:

1) Public Cloud

A public cloud is a kind of figuring wherein a specialist co-op makes assets accessible to the public through the web. Assets fluctuate by supplier however may incorporate capacity abilities, applications, or virtual machines. Public cloud takes into account adaptability and asset sharing that would not, in any case, be workable for a solitary association to accomplish. Public cloud is possessed and facilitated worked by a cloud merchant, which conveys their workers and capacity over the Internet. AWS, V cloud, Google Cloud and Microsoft Azure is an illustration of a public cloud. With a public cloud, a total framework is claimed and overseen by the cloud supplier. You access these things utilizing web support.

2) Private Cloud

A private cloud is a processing model that offers a restrictive control devoted to a solitary business substance. Likewise, with different sorts of Cloud computing conditions, a private cloud gives broadened, virtualized registering assets by means of actual segments put away on-premises or at a seller's datacenter. A private cloud alludes to Cloud computing assets utilized by one organization. A private cloud can be genuinely situated in the organization. A few organizations additionally utilize an outsider assistance merchant to have their cloud. A private cloud is one in which the foundation is kept up on a private own organization.

3) Hybrid Cloud

A hybrid cloud is a cloud that consolidates a private cloud with at least one public cloud administrations, with restrictive programming empowering correspondence between each particular help. A hybrid cloud procedure furnishes organizations with more noteworthy adaptability by moving responsibilities between cloud arrangements as necessities and expenses change. By permitting information and applications to move among private and public clouds, gives our business extraordinary opportunity and arrangement alternatives and assists with getting our foundation all the more productively.

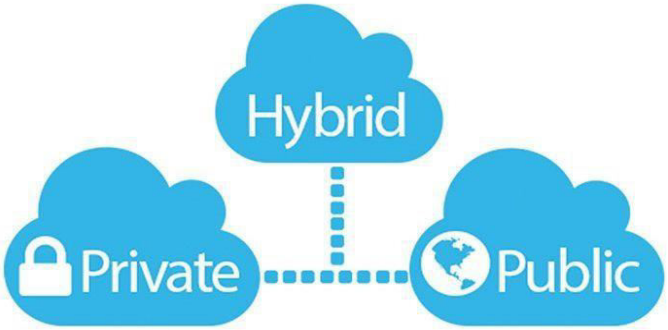

Fig -1: Hybrid Cloud

3.Types of cloud computing services:

1) Infrastructure as a Service

The most essential assistance of the cloud is IaaS. In the IaaS model, the cloud supplier oversees IT frameworks like stockpiling, worker, and systems administration assets, and conveys them to supporter associations by means of virtual machines available through the web. IaaS can have numerous advantages for associations, for example, possibly making jobs quicker, simpler, more adaptable, and more expense effective. On compensation, as u use premise with IaaS, we can lease IT foundation workers and virtual machines (VMs), stockpiling, organizations, working frameworks from a cloud seller.

2) Platform as a Service

PaaS is a sort of Cloud computing offering in which a specialist co-op conveys a stage to customers, empowering them to create, run, and oversee business applications without the need to assemble and keep up the framework such programming advancement measures regularly require. Stage as administration supplies an on-request climate for creating, testing, conveying, and overseeing programming applications. PaaS is intended to make it simpler for engineers to rapidly

make an application or site, without stressing over the foundation.

3) Software as a Service

SaaS permits clients to associate with and use cloud-based applications over the Internet. Regular models are email, calendaring and office devices, (for example, Microsoft Office 365). Programming as a help is a strategy for conveying programming applications over the Internet. With SaaS, cloud suppliers have and deal with the product application and will deal with the upkeep of that product like redesigns security of the product, and so on Client's interface with the application over the Internet utilizing their gadget.

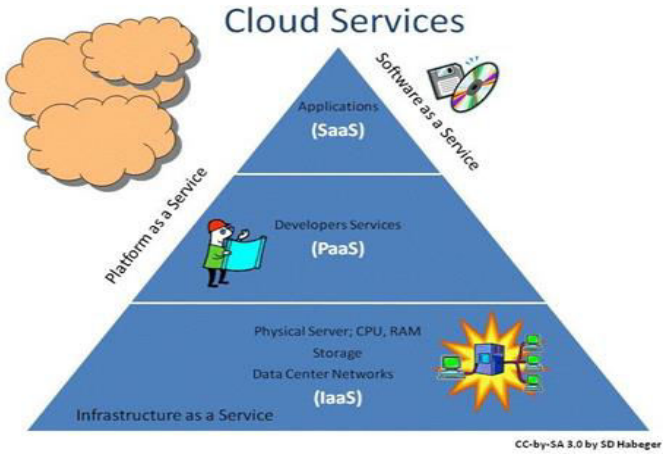

Fig -2: Cloud Services

4.Benefits of Cloud Computing:

1) Cost efficient to build an infrastructure
2) Dependable performance
3) Less Maintenance issues
4) Regular Software Updates
5) Improved compatibility between systems
6) Easy backup and recovery
7) Performance and Scalability
8) Increased storage capacity

5.Cloud Architecture:

Cloud computing involves two parts front end and back end. The front end comprises customer some portion of a Cloud computing framework. It involves interfaces and applications that are needed to get to the cloud stage. While the back end alludes to the actual cloud, it involves the assets that are for Cloud computing administrations.

It comprises of VMs, workers, stockpiling, security units, and so forth It is heavily influenced by a cloud supplier. Cloud computing disperses the record framework that spreads over numerous hard circles and machines. Information is never put away in one spot just and on the off chance that one unit bombs the other will take over naturally. The client circle space is dispensed on the circulated document framework.

6.Security Concerns in Cloud:

The significant issue that emerges in the client's mind is its security. One concern is that cloud merchants themselves may approach the organization's decoded information whether it's on disk, in memory, or the information that movement over the organization.

To give security to frameworks, organizations, and information, cloud computing specialist co-ops have held hands with TCG (Trusted Computing Group) which is a non-benefit association that consistently delivers a bunch of rules to get equipment, make self-encoding drives, and improve security. It shields the information from unapproved access and ensures that information is protected.

As registering includes various gadgets like hard plate drives and cell phones, TCG has stretched out the safety efforts to incorporate these gadgets to ensure that clients are protected.

6.Privacy in Cloud

Privacy presents a strong barrier for users to adapt into Cloud Computing systems. There are certain measures which can improve privacy in cloud computing.

The authoritative staff of the Cloud computing administration could hypothetically screen the information moving in memory before it is put away on a disk. To keep the secrecy of information, authoritative and legitimate controls ought to keep this from occurring.

Here to ensure the information is classified, cryptographic calculations and a solid confirmation cycle ought to be utilized. Furthermore, encryption of the information is an unquestionable requirement, here encryption implies putting away information in the cloud so that lone approved clients can comprehend and get to that specific information. Appropriate encryption is incredible to the point that even the cloud specialist organization will be not able to peruse the information.

7.Security Concerns in Cloud Computing:

1)Issues during transfer of data to the cloud

It is the way toward moving information over a medium to at least one figuring organization. In a Cloud environment, a large portion of the information isn't scrambled in the preparing time. To deal with information for any application that information should be decoded. Information theft when the assailants place themselves in the interchanges way between the clients. Here there is the likelihood that they can hinder and change correspondences to their ideal locations.

2)Security issues in the Virtual Machines

Virtual Machine (VM) implies sharing the assets of a solitary actual PC into different PCs. VM's give readiness, adaptability, and versatility to the cloud assets by permitting the cloud specialist organizations to duplicate, move and control their VM's. Remembering this, vindictive programmers are discovering approaches to get their hands on information by penetrating the security layers of cloud conditions. The Cloud computing situation isn't pretty much as straightforward as it professes to be. The assistance client has no clue about how the information is handled and put away. Also, don't have direct command over the progression of information.

3)Issues with the Application Programming Interface
Clients deal with and collaborate with cloud benefits through API's. Cloud specialist organizations should guarantee that security is incorporated into their administration models, while clients should know about security hazards.

8.Solution for Security Issues in Cloud:

Cryptography in the cloud utilizes encryption methods to get information that will be utilized or put away in the cloud. It permits clients to helpfully and safely access shared cloud administrations, as any information that is facilitated by cloud suppliers is secured with encryption. Cryptography in the cloud secures delicate information without deferring data trade. Cryptography in the cloud takes into consideration getting basic information past your corporate IT climate, where that information is not, at this point under your control. The advantages of Cloud computing are being acknowledged by more organizations and associations consistently.

Cloud computing gives customers a virtual figuring framework on which they can store information and run applications. But Cloud computing has presented security challenges in light of the fact that cloud administrators store and handle customer information outside of the scope of customers' current safety efforts.

Different organizations are planning cryptographic conventions custom-fitted to Cloud computing trying to viably adjust security and execution. Most Cloud computing foundations don't give protection from untrusted cloud administrators, which represents a test for organizations and associations that need to store touchy, classified data like clinical records, monetary records, or high-sway business information.

As Cloud computing keeps on filling in prominence, there are many Cloud computing organizations and specialists who are seeking after cloud cryptography projects to address the business requests and difficulties identifying with cloud security and information assurance. There are different ways to deal with stretching out cryptography to cloud information. Numerous organizations decide to encode information before transferring it to the cloud inside and out.

This methodology is valuable since information is scrambled before it leaves the organization's current circumstance, and information must be unscrambled by approved gatherings that approach the proper decoding keys. Other cloud administrations are equipped for scrambling information upon receipt, guaranteeing that any information they are putting away or sending is secured by encryption of course. Some cloud administrations may not offer encryption abilities, yet in any event should utilize encoded associations, for example, HTTPS or SSL to guarantee that information is gotten on the way.

9.Cryptographic Algorithms:

There are multiple Cryptographic algorithms that are implemented today. Few examples are:

1)Attribute based Encryption
This is a public key encryption. It also produces a secret key which has a list of attributes. After every transaction a new attribute list is formed. If the user has the same set of attributes, then access is granted. This algorithm is a basic algorithm which is implemented in our everyday applications. This algorithm is not very efficient as it does not provide proper security but it is user friendly.

2)Fully Homomorphic Encryption Algorithm
The most advanced algorithm that is in much demand currently is the Fully decryption on cipher texts. The operations of cloud computing are directly done on the cipher text, which when decrypted produces the same output as our daily plain text. New patterns and sequences are generated after fixed intervals with certain number of transactions. This is strongest algorithm which running currently. It is privacy-preserving. this allows data to be encrypted and out-sourced to commercial cloud processing. This also helps in implementing privacy barriers which prevents the data being shared to any other system. It is very difficult for hackers to crack this code. There are multiple generations of this code. First generation only uses lattice-based cryptography which performs basic operations on low degree polynomials. Second generation code are basically derived from numerous algorithms, which form a complete homomorphic system but is overstretched with a lot of unused variants. Third generation techniques were further improved in removing the ring variants. This algorithm refreshes the cipher text after every single operation, it is possible to reduce the bootstrapping time to a fraction of a second.

3)Signal Control Encryption
Signal protocol for encryption, which utilizes a mix of asymmetric and symmetric key cryptographic calculations. The symmetric key calculations guarantee secrecy and Integrity while the uneven key cryptographic calculations help in accomplishing the other security objectives to be specific validation and non-renouncement. In symmetric-key cryptography, a primary key is utilized for encryption of the information just as cryptography. In asymmetric key cryptography, there would be two separate keys. The information which is encoded utilizing the public key of a client must be decoded utilizing the private key of that client and the other way around.

4)Hash function
A cryptographic hash work doesn't utilize keys for its essential activity. This capacity makes a little review or "hash value" from regularly a lot of information through a single direction measure. Hash capacities are by and large used to make the structure impedes that are utilized in key administration and give security administrations, such as:
1.Providing source and integrity authentication services by generating message authentication codes (MACs).
2.Compressing messages for generating and verifying digital signatures
3.Deriving keys in key-establishment algorithms
4.Generating deterministic random number

5)Symmetric Key Encryption
Also referred to as secret key calculation, a symmetric-key calculation changes information to make it incredibly hard to see without having a secret key.

The key is considered symmetric on the grounds that it is utilized for both encryption and decryption. These keys are typically known by at least one approved element. Symmetric key calculations are utilized for:
1)Providing data confidentiality by using the same key for encrypting and decrypting data.
2)Providing Message Authentication Codes (MACs) for source and integrity authentication services. The key is used to create the MAC and then to validate it.
3)Establishing keys during key-establishment processes
Generating deterministic random numbers.

6)Asymmetric Key Encryption
Also referred to as public-key algorithms, asymmetric-key algorithms use paired keys (a public and a private key) in performing their function. The public key is known to all, but the private key is controlled solely by the owner of that key pair. The private key cannot be mathematically calculated through the use of the public key even though they are cryptographically related. Asymmetric algorithms are used for:
1)Computing digital signatures
2)Establishing cryptographic keying material
3)Identity Management

3. CONCLUSIONS

In today's world cloud computing is an essential technology where each and every organization are moving towards cloud but the major fear that is running in users mind is about the security of their data.
Usage of Cryptography for securing data in organization will reduce the security issues in cloud and also from the clients there should be a proper legal agreement to be done with the cloud provider before the setup of cloud in the organization. And also, an active and efficient team need to be working on encryption of data before storing or transferring the data to the cloud.

ACKNOWLEDGEMENT

REFERENCES

1. V.Suresh Babu , Maddali M.V.M kumar
– "An efficient and secure data storage operations in cloud computing". – 2018 IJSRSET volume 4. Themed section: engineering and technology.
2. Supriya D Patil, Komal S Talekar,Reshma R Raskar,Pooja A Chavans –"Attribute based access control in personal health records using cloud computing – 2018 IRJET volume 4.
3. Vivek paul , Supriya Panditha – "Cloud computing review" – Mar 2018 IRJET volume 5.
4. A Venkatesh , Marrynal S Eastaff – "A Study of data storage issues in cloud computing" – 2018 IJSRCSEIT volume 3.
5. M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: From single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.
6. E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014.