MONITORING AND DETECTION OF SECURITY VIOLATIONS ON CLOUD STORAGE

[1]Femenca Noronha, [2]Suman Gupta
[1]Student, [2] Student
[1]IT Department,
[1]Thakur College of Science &Commerce, Kandivali East, Mumbai – 400101, Maharashtra, India

Abstract : Today, cloud computing is where all look up to and that is because of the convenience it has given the users, in terms of monetary benefits, space, place management, flexibility which the users can rejoice on, efficiency and the strategic value it provides to the organization and the users. With the benefits mentioned above; greatest add on is the security the data stored is stored with. There are several advantages that the users enjoy in cloud computing but there are some pitfalls (security issues) too. The main objective of this paper is to highlight those security issues and the successful monitoring of those issues.

Keywords: *Cloud computing; Violations ; Monitoring; Security.*

I. INTRODUCTION

Cloud computing is the act of utilizing a facilitated system of remote servers on the Internet to store, oversee, and process information, as opposed to a neighborhood server or a PC. It is a sort of Internet based figuring component that gives shared PC handling assets and information to PCs and different gadgets on interest. Distributed computing Technology and the capacity arrangements furnish clients and ventures with different abilities to store and process their information in either exclusive, or by the outsider server farms that might be situated a long way from the client going in separation from over a city to over the world.

There are a few distinct types of administration models that can be utilized in the cloud innovation by cloud specialist organizations. It incorporates programming, frequently alluded to as Software as a Service (SaaS), and for advancement and facilitating of use with no intricacy of upkeep of its framework is regularly referred to as Platform as a Service (PaaS) and furthermore a whole systems administration foundation based administration instrument referred to as Infrastructure as a Service (IaaS).
Though we are worried about the expression "Data security" that is one of the serious issues landing in cloud computing which develops the idea of shielding the information and data frameworks from all the unapproved divulgence, disturbance, change, or annihilation.

In any case, clients have a constrained perspective on the security and can demand more straightforwardness with systems that give administration security ensures.

1.1 SERVICE MODELS

As per NIST, the cloud model is composed of three service models:

- **Software as a Service (SaaS)**: The capability provided to the customer is to utilize the provider's applications running on a cloud foundation. The applications are open from different customer gadgets through either a dainty customer interface, for example, an internet browser (e.g., electronic email), or a program interface. The customer does not oversee or control the basic cloud framework including system, servers, working frameworks, stockpiling, or even individual application abilities, with the conceivable exemption of restricted client explicit application design settings [4].

- **Platform as a Service (PaaS):** The capability given to the customer is to convey onto the cloud foundation where the customer applications are made utilizing programming dialects, libraries, administrations, and instruments upheld by the provider. The customer does not oversee or control the basic cloud foundation including system, servers, working frameworks, or capacity, yet has power over the conveyed applications and conceivably design settings for the application-facilitating condition [4].

- **Infrastructure as a Service (IaaS)**: The capability given to the customer is to arrange and prepare the systems in such a way where the customer can convey and run self-assertive programming, which can incorporate working frameworks and applications. The customer does not oversee or control the fundamental cloud framework but rather has authority over working frameworks, stockpiling, and sent applications; and conceivably constrained control of select systems administration segments (e.g., host firewalls) [4].

1.2 DEPLOYMENT MODELS:

There are four cloud deployment models mentioned in [2] as following:

- **Private cloud:**

In this model, the cloud provider provides cloud infrastructure to a single organization that has many consumers. The private cloud infrastructure is to be used exclusively for their use and need. The owner, manager, and operator of this cloud could be the organization itself, a third party, or the organization and third party together. This private cloud could be on premises or off premises.

- **Community Cloud:**

In this model, the cloud provider provides cloud infrastructure to many organizations that forms community that shares mission, security requirements, compliance consideration, or policy. The community cloud infrastructure is to be used exclusively for their uses and needs. The owner, manager, and operator of this cloud could be one of organizations, a third party, or the organization and third party together. This Community cloud could be on premises or off premises.

- **Public Cloud:**

This model is completely different from the previous model in that it is open for the public; it is not private and not exclusively for community. In this model, a public cloud can be provisioned for public to use it to satisfy their needs. The owner, manager and operator of this cloud could be a government, private organization, a business or academic organization, and sometimes many of them can be in one cloud and get the service from the same provider.

- **Hybrid Cloud :**

The hybrid cloud model consist of two or more deployment models (private, community, or public). The cloud infrastructure can be combination of those models. Data center within an organization, private cloud, and public cloud can be combined in order to get services and data from both in order to create a well-managed and unified computing environment. A cloud can be considered hybrid if the data moves from a data center to a private cloud or public cloud or vice versa.

II. PROBLRM STATEMENT

Whenever somebody needs to store any of their information anyplace on the cloud the serious issue that emerges is the security of that information which incorporates the four essential key standards of security that is confidentiality, integrity, confirmation and non-repudiation. Hence a safe domain is must for the clients so as to store their information. The principle goal of the data framework is to fill its need; the data must be accessible when it is required. This implies the figuring framework should store and process the data, while the security controls must assistance in ensuring it, and the correspondence channels that have been utilized to get to the data must capacity accurately.Thus, a safe domain is must for the clients so as to Store their information on the cloud. Cryptography is one such technique to provide confidentiality and also to prevent data leakage. However, some attacks, performed by malicious users cannot detected, resulting in security violations. Thus, it is necessary to monitor and audit a cloud service in order to identify these violations.

III. CURRENT METHODOLOGY

Researchers have been proposed to security instrument by utilizing the cryptography methods. That is tied in with structuring, building and investigating a few conventions that anticipate the outsiders or people in general from getting to the private information. Different viewpoints in data security, for example, information privacy, information trustworthiness, validation, and non-disavowal are considered as the focal way to deal with current cryptography.

Security instruments must be intended to ensure a client against existing dangers, holding the mentioned security properties. In this examination, we break down the classification, trustworthiness, retrievability, freshness and compose serializability of the information put away in the cloud. The classification and uprightness are basic to keep away from the information access or information change by unapproved clients. The retrievability is identified with the information misfortune check, and the freshness shows the perusing of the refreshed record. The compose serializability controls the composition request, guaranteeing that the new form of a record overwrites the last form of it [16].

When it comes to cryptography, encryption is the process of encoding information in such a way that only authorized users and systems can access it. Cloud Storage are always responsible for the encryption of your data on the server side, before it is written to disk, at no additional charge. Besides this standard behavior, there are more different ways to encrypt your data while using Cloud Storage. encryption that occurs after Cloud Storage receives your data, but before the data is written to disk and stored [14]. An authorized receiver can easily decrypt the message with the key provided by the sender to the receiver, but no unauthorized and the third party interceptors will be allowed or able to decrypt that message.

When you perform customer side encryption, you should make and deal with your very own encryption keys, and you should utilize your own instruments to scramble information before sending it to Cloud Storage. Information that you encode on the

customer side touches base at Cloud Storage in a scrambled state, and Cloud Storage has no learning of the keys you used to scramble the information.

At the point when Cloud Storage gets your information, it is encoded a second time. This second encryption is called server-side encryption, which Cloud Storage oversees. When you recover your information, Cloud Storage evacuates the server-side layer of encryption, yet you should unscramble the customer side layer yourself. [3]

The data security in the cloud data involves a number of tools, technologies and approaches. There are several advantages when it comes to the cloud one of such is that many security elements are already built into cloud systems. This typically includes strong encryption at rest and in motion. It may also involve:

- **Geo-fencing** -The utilization of IP addresses and other geo-location information to make a geographic limit and recognize suspicious action.
- **Policy-based lifecycle retention**-Frameworks use information arrangement polices to oversee and computerize how information is put away, held, documented and erased.
- **Data-aware filtering** - This capacity enables associations to look for explicit conditions and occasions – and who has gotten to data and when they got to it. It very well may be attached to job based approvals and benefits.
- **Detailed logs and full user/workload audit trail reporting -** The capacity to look into logs and review remaining burdens can give knowledge into security concerns and helplessness dangers.
- **Backup and recovery functions** - These fundamental capacities enable an association to explore a blackout yet in addition manage security dangers, for example, ransomware assaults and vindictively erased information. Strong cloud-based debacle recuperation arrangements prompts accessibility over all conditions [11].

The access control and key administration mechanisms give the classification and document sharing. In the security assessment of this mechanism, it is exhibited that unapproved clients can't get the keys, guaranteeing the classification. Then again, the integrity verification performed by existing mechanisms isn't sufficient to recognize infringement of access control in light of the fact that a repudiated client can compose new documents utilizing old accreditations, which might be considered legitimate. Therefore, it is necessary the access control verification although no found solution verifies these violations [16].

IV. PROPOSED WORK

So as to keep up the security in cloud storage Embedding cryptography with steganography could be a great approach. Cryptography can give us the security by scrambling the information just as data before transferring it to the distributed storage though when once the information is transferred on cloud, Steganography will give security by concealing the presence of information and data being imparted [9].

Along with the above proposed method to secure data on cloud storage we propose to make use of the RAID-technology principle to manage data distribution across cloud storage providers.

Using Cloud-RAID, a framework would improve the availability, confidentiality and integrity of information put away on the cloud. To accomplish this target, we encode client's information and utilize the RAID-innovation rule to oversee information appropriation crosswise over distributed storage suppliers [7]

RAID-based storage systems are essentially inefficient, especially at cloud-scale proportions. In order to maintain data integrity and availability to large user bases, a typical cloud storage infrastructure using a RAID-based system would have to create multiple copies of each data set and distribute those across multiple storage systems - even multiple data centers. This process, generally called “replication” can take several forms, from simply copying an entire volume between arrays to more sophisticated object-level replication [8].

4.1 DETECTION MODULES

- **Access Control Lists:**

It is used to specify users’ permissions and is capable to work together with the others security mechanisms. Besides, Broadcast Encryption and Key Rotation are efficient mechanisms to, respectively, distribute and update the reading and writing keys [11]. Thus,

the provider stores the metadata of each file to enable the authorized users to extract the reading or writing credentials. Besides, metadata includes the tag used for retrievability and verification.

- **Monitoring of Cloud Transactions Logs:**

The elements of an monitoring the logs include the following user's data: UserID, UserLSN, FileID, FileVersion, FileHash, TransactionType, KeyVersion, ChainHash and Signatures [11].

- **Entity Detection:**

The entity detection is used for detecting the entities which are responsible for generation of traffic for attack. Whenever there is a new flow of such traffic on the network the entities receive the informations regarding same. Thus those information can be extracted and the attack can be detected [12].

- **Entity Validation:**

The evaluation of entity validation deals with various tasks such as buffer overflow, URL redirection and injection attacks. Critical files and invalid inputs or outputs can be accessed and detected using entity validation Monitoring technique.

- **Studying the report generated:**

This include generation of a report file which will include various informations such as time, type of communication, total number of bytes and packets transferred between the source and the destination systems. Thus, a study of such report can successfully exploit the attacker and the violations that has taken place by using the informations been generated in the report [12].

V. CONCLUSION

For assuring the security of the data on a distributed cloud storage, effectively different mechanisms have been utilized and actualized by the scientists which incorporate the encryption and the unscrambling of the information that must be put away on cloud. This security can be increasingly improved by utilizing the steganography strategies with the cryptography component. We have summarized the enhancement of the cloud security using the RAID integration on the cloud data. This proposal describes a secure cloud storage service, along with enhanced security mechanisms such as maintaining confidentiality, integrity, retrievability, freshness and write-serializability of data stored and shared on the cloud.

Some detection modules has also been proposed which will ensure that the data on the cloud is secure and in case the data is violated it can be detected on time using the above mentioned detection modules and proper actions can be taken.

In this paper overall we have summarized the service models in the cloud computing technology and also highlighted the issues arising for the users regarding the security of their data in the cloud storage with proper proposed detection mechanisms.

REFERENCES

[1]. Oktay Tontaş, J. Bernardino, "*The Ethics in Cloud Computing"*; 2nd International Conference of the Portuguese Society for Engineering Education (CISPEE), 2016.
[2]. Sultan Aldossary, Prince Sattam Bin Abdulaziz , "*Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions "*(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016
[3]. https://cloud.google.com/storage/docs/encryption/client-side-keys
[4]. Peter Mell. (2011) 'The NIST Definition of Cloud ', Reports on Computer Systems Technology, sept., p. 7.
[5]. Mrinal Kanti Sarkar, Sanjay Kumar, *"A Framework to Ensure Data Storage Security in Cloud Computing"*, ISBN-978-1-5090-1496-5, 2016.
[6]. Maxim Schnjakin, Christoph Meinel "Implementation of Cloud-RAID: A Secure and Reliable Storage above the Clouds" International Conference on Grid and Pervasive Computing GPC 2013: Grid and Pervasive Computing pp 91-102
[7]. Mohit Marwaha**,** Rajeev Bedi**, "***Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing"***,** IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.
[8]. http://www.storage-switzerland.com/Articles/Entries/2013/3/4_A_Better_Answer_than_RAID_and_Replication_for_Cloud_Storage.html.

[9]. Kazuki Murakami, Qiangfu Zhao, Ryota Hanyu, *"A New Steganography Protocol for Improving Security of Cloud Storage Services"*, ISBN-978-1-4799-4476-7, 2014.

[10]. https://en.wikipedia.org/wiki/Cryptography

[11]. R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang,"Enabling security in cloud storage slas with cloudproof," in Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference, USENIXATC'11, 2011.

[12]. Vijay Varadharajan and Udaya Tupakula,"*Securing Services in Networked Cloud Infrastructures*" IEEE Transactions on Cloud Computing DOI 10.1109/TCC.2016.2570752

[13]. Shakeeba S. Khan, Prof.R.R. Tuteja ,*"Security in Cloud Computing using Cryptographic Algorithms"*, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.

[14]. https://cloud.google.com/storage/docs/encryption/

[15]. MSIT-121C (Elective 2): Cryptography and Network Security, pg.27-29. http://164.100.133.129:81/eCONTENT/Uploads/MSIT121C-Cryptography_and_Network_Security.pdf

[16]. Carlos Andre Batista de Carvalho, Miguel Franklin de Castro and Rossana Maria de Castro Andrade "*Secure cloud storage service for detection of security violations*" , 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing