Cloud Data Security Using Cryptography: A Review

Tayyeba Aaliya[1], Rahul Sharma[2]
[1, 2] Dept of Computer Science
[1, 2]RKDF School Of Engineering

Abstract- *Cloud computing is a new and rapid growing technology. In present days cloud computing is one of the greatest platform which provides storage of data in very lower cost and available for all time over the internet. But there is a big problem of security in cloud computing. In the context the security and privacy management is essential for cloud computing. In this survey papers we introduce the cloud security issues and recently developed method which is used concept of homomorphic and split key data encryption. Further this helps to find out the solution for the drawbacks found in given literature and come up with new solution or method to secure the cloud.*

Keywords- cloud computing, security and privacy issues, cryptographic system, and data preservation.

I. INTRODUCTION

This We are increasingly relying on a number of online file storage systems to back up our data or use it as a collaborative tool in real time. All these services bring with it a fair share of security and privacy vulnerabilities for all the conveniences provided by them. Security has always been the main issue for IT Executives when it comes to cloud adoption. With developing mindfulness and concerns respects to Cloud Computing and Information Security, there is developing mindfulness and use of Security Algorithms into information frameworks and procedures. From the point of view of information security in cloud, this has dependably been an essential part of nature of administration. The information put away in the cloud might be every now and again refreshed by the clients, including inclusion, erasure, and change, annexing, reordering, and so forth. To guarantee stockpiling accuracy under powerful information refresh is henceforth of vital significance [1].

Information is a key resource for any association. Information could be in any structures, i.e. numbers, words, pictures and so on. Information protection and security is a vital issue for any association. Information manages different properties, for example, precision, legitimacy, unwavering quality and so on depicted underneath [2].

A. Cloud Storage

Cloud storage is composed of thousands of storage devices clustered by network, distributed file systems and other storage middleware to provide cloud storage service for users. The typical structure of cloud storage includes storage resource pool, distributed file system, service level agreements (SLA), and service interfaces, etc. Globally, they can be divided by physical and logical functions boundaries and relationships to provide more compatibilities and interactions. Based on this idea, the architecture proposed here are as follows. It is a layered model. The architecture from bottom to upper is network and storage infrastructure, storage management, metadata management, storage overlay, service interface. The detailed functions will be discussed later [3].

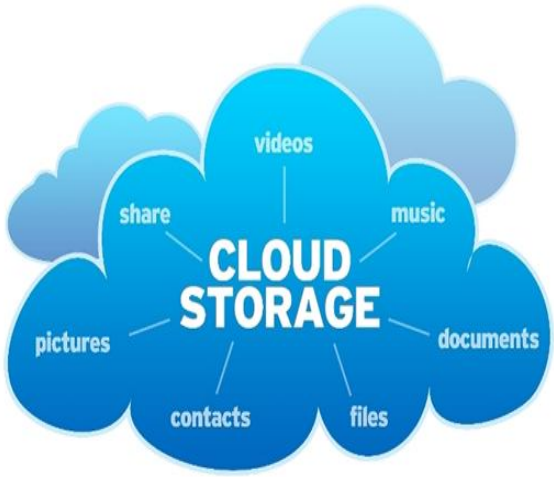

Figure 1: Cloud Storage

A. Features of Cloud Storage

Most of the services are free up to certain number of gigabytes, and storage also. The entire cloud provider provides all the features to the end user like drag and drop, syncing files and folder in your desktop, mobile device and soon [4].

Advantages:

- ✓ *Usability* – the cloud provider are always usable at any time.
- ✓ *Bandwidth* – avoid of sending the files to individual instead of send a web link to the end user through email it.

- ✓ *Accessibility* – stored files and folder are accessible from any were in cloud platform
- ✓ *Disaster Recovery* – back up facility should be there in cloud storage which is helpful for the businesses. Back up the data should be more important in electronic medium. Backup files are remotely stored and access through internet connection
- ✓ *Cost Savings* – In cloud storage 3 percent gigabyte are there to store data internally. Businesses and organizations reduce the cost by using cloud storage. Data are stored remotely on it.

Disadvantages:

- ✓ *Usability* – Be carefully of using the drag and drop option which is used in cloud storage that will permanently remove your file. While using drag and drop option used the copy and paste option to it which will save your files from the permanent delete.
- ✓ *Bandwidth* – limited bandwidth allowed in the cloud storage. If you want more bandwidth then it should be payable. However, some providers have unlimited bandwidth on it.
- ✓ *Accessibility* – to access the data and files you need an internet connection. With-out it not possible.
- ✓ *Data Security* – Data should be safely and privately stored on the cloud storage.
- ✓ *Software* – if you want to access your file locally then you need to download all the services on that devices.

Cloud storage is composed of thousands of storage devices clustered by network, distributed file systems and other storage middleware to provide cloud storage service for users. The typical structure of cloud storage includes storage resource pool, distributed file system, service level agreements (SLA), and service interfaces, etc. Globally, they can be divided by physical and logical functions boundaries and relationships to provide more compatibilities and interactions. Based on this idea, the architecture proposed here are as follows. It is a layered model. The architecture from bottom to upper is network and storage infrastructure, storage management, metadata management, storage overlay, service interface. The detailed functions will be discussed later [3].

A. Issues in Cloud Storage

It is the duty of cloud service provider to make sure that the customer does not face any problems. Like any other technology cloud computing also suffers some problems. As it is a great promise to the future, it is necessary to understand about the issues related to the cloud computing technology. Some of the major issues suffered by this technology are [5] [6]:

Trust

Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intention or behaviour of another. It is an expansion of security in cloud computing technology and is divided into two categories: Hard Trust, and Soft Trust. Hard trust is security oriented and Soft trust is non-security oriented. If we have control over the systems we can trust the system. Trust is defined as the integrity, strength, ability and surety of a person or a thing. The cloud service provider must achieve the trust of the customers by providing trustworthy services. If any incidents like hacking or crashed service will certainly create some doubts in customer's mind and their trust in service provider will be damaged.

Privacy

Cloud computing is not like the traditional computing model, as it utilizes the virtual computing technology. User's personal data are scattered in various virtual datacentres, which even cross the national borders. So the chance of data leakage is so high and the attackers can easily access the private data.

Security

Security is the main issue in cloud computing. Security must be done on two levels: user level and provider level. The service provider should make sure that the server is well secured from all threats. Even though the service provider provides good security for the user, the user should make sure that there are no threats to their data

II. BACKGROUND

The background of a study is an important part of our research paper. It provides the context and purpose of the study. Hence there is need for background study that contribute to prepare proposed system.

A. Cloud Cryptography and Security

Cryptography in the cloud utilizes encryption methods to secure information that will be utilized or put away in the cloud. It enables clients to advantageously and safely get to shared cloud administrations, as any information that is facilitated by cloud suppliers is ensured with encryption.

Cryptography in the cloud secures delicate information without postponing data trade [7].

There are various approaches to extending cryptography to cloud data. Many companies choose to encrypt data prior to uploading it to the cloud altogether. This approach is beneficial because data is encrypted before it leaves the company's environment, and data can only be decrypted by authorized parties that have access to the appropriate decryption keys. Other cloud services are capable of encrypting data upon receipt, ensuring that any data they are storing or transmitting is protected by encryption by default. Some cloud services may not offer encryption capabilities, but at the very least should use encrypted connections such as HTTPS or SSL to ensure that data is secured in transit [8].

B. Cloud Encryption and Crypto Management

Organizations and associations need to adopt information driven strategy to ensuring their delicate data with a specific end goal to make preparations for cutting edge dangers in the complex and developing situations of virtualization, cloud administrations, and portability. Organizations should actualize information security arrangements that give steady insurance of touchy information, including cloud information assurance through encryption and cryptographic key administration. A complete stage for cloud security and encryption additionally ought to convey powerful access controls and key administration capacities that empower associations to for all intents and purposes, cost viably, and exhaustively use encryption to address security targets [8].

C. Cryptographic Cloud

All data is pre-processed by a client device before being uploaded to the cloud; the pre-processing signs and encrypts the data in such a way that its functionality is preserved, allowing, for example, for the cloud to search or compute over the encrypted data and to prove its integrity to the client (without the client having to download it). We refer to this type of solution as Cryptographic Cloud Storage.

Cryptographic cloud storage is achievable with current technologies and can help bootstrap trust in public clouds. It can also form the foundation for future cryptographic cloud solutions where an increasing amount of computation on encrypted data is possible and efficient.

D. Application of the Cryptographic Cloud

Storage services based on public clouds such as Microsoft's Azure storage service and Amazon's S3 provide customers with scalable and dynamic storage. By moving their data to the cloud customers can avoid the costs of building and maintaining a private storage infrastructure, opting instead to pay a service provider as a function of its needs. For most customers, this provides several benefits including availability (i.e., being able to access data from anywhere) and reliability (i.e., not having to worry about backups) at a relatively low cost. While the benefits of using a public cloud infrastructure are clear, it introduces significant security and privacy risks. In fact, it seems that the biggest hurdle to the adoption of cloud storage (and cloud computing in general) is concern over the confidentiality and integrity of data [9].

While, so far, consumers have been willing to trade privacy for the convenience of software services (e.g., for web-based email, calendars, pictures etc.), this is not the case for enterprises and government organizations. This reluctance can be attributed to several factors that range from a desire to protect mission-critical data to regulatory obligations to preserve the confidentiality and integrity of data. The latter can occur when the customer is responsible for keeping personally identifiable information (PII), or medical and financial records.

In addition to simple storage, many enterprises will have a need for some associated services. These services can include any number of business processes including sharing of data among trusted partners, litigation support, monitoring and compliance, back-up, archive and audit logs. A cryptographic storage service can be endowed with some subset of these services to provide value to enterprises, for example in complying with government regulations for handling of sensitive data, geographic considerations relating to data provenance, to help mitigate the cost of security breaches, lower the cost of electronic discovery for litigation support, or alleviate the burden of complying with subpoenas [9].

For example, a specific type of data which is especially sensitive is personal medical data. The recent move towards electronic health records promises to reduce medical errors, save lives and decrease the cost of healthcare. Given the importance and sensitivity of health-related data, it is clear that any cloud storage platform for health records will need to provide strong confidentiality and integrity guarantees to patients and care givers, which can be enabled with cryptographic cloud storage

Another area where a cryptographic cloud storage system could be useful is interactive scientific publishing. As scientists continue to produce large data sets which have broad

value for the scientific community, demand will increase for a storage infrastructure to make such data accessible and sharable. To invent scientists to share their data, scientific could establish a publication forum for data sets in partnership with hosted data centers. Such an interactive publication forum would need to provide strong guarantees to authors on how their data sets may be accessed and used by others, and could be built on a cryptographic cloud storage system.

III. LITERATURE SURVEY

This section introduces the prior work done and research work solutions in cloud data security using different encryption technique. Some of the research work papers are listed here:

The SecCloud is displayed by **Wei et al. [10],** it gives a capacity security convention to cloud client's information and it secures the put away information as well as gives security on computational information. The SecCloud convention utilizes encryption for putting away information in secure mode. The multiplicative gatherings and cyclic added substance matching is utilized for key age for cloud clients, CSP, and different business accomplices or trusted outsider. The encoded information along with the obvious mark is sent to cloud server farm alongside session key. The Diffie-Hellman calculation is utilized for age of session key for both bilinear gatherings. By getting encoded information the cloud decodes the information, checks the computerized mark and stores the first information in indicated area in cloud. The SecCloud checks regardless of whether information is put away at determined area or not. The Merkle hash tree is utilized for calculation security in SecCloud convention. The confirming organization will check the computational outcomes that are working by utilizing Merkle hash tree.

The Purpose of homomorphic encryption is to guarantee security of information in correspondence, stockpiling or being used by forms with instruments like regular cryptography, yet with included capacities of registering over scrambled information, looking through encoded information, and so on. Homomorphism is a property by which an issue in one logarithmic framework can be changed over to an issue in another arithmetical framework, be explained and the arrangement later can likewise be deciphered back viably. Along these lines, homomorphism makes secure designation of calculation to an outsider conceivable. Numerous traditional encryption plans have either multiplicative or added substance homomorphic property and are presently being used for particular applications. **Kamal Benzekki et al. [11]** propose a multi-cloud design of N circulated servers to repartition the information and to almost permit accomplishing a FHE.

When the data transferred to the Cloud we use standard encryption methods to secure the operations and the storage of the data. But to process data located on a remote server, the Cloud providers need to access the raw data. In this paper **Maha TEBAA et al. [12]** are proposing an application of a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if authors have worked directly on the raw data.

To keep client information classified from an untrusted Cloud Service Provider and outsiders, a characteristic way is encryption. The information unscrambling key ought to be revealed just to clients who have been approved. Clients can look through their documents utilizing watchwords in the cloud. In existing writing many plans have been proposed. In this paper **R. Sharmila et al. [13]** depicted another system: Multi-watchword seeking utilizing homomorphic encryption. It is a calculation which performs operations on scrambled information which will give comes about without unscrambling that information. It gives protection to client questioning examples and client information. It permits Cloud Service Providers to perform operations on the encoded information. The Cloud Service Provider is unconscious of the documents and watchwords put away in the cloud. Positioning is utilized for proficient and quick recovery of the coveted records. Positions will be doled out to records in view of the recurrence of access of the documents.

Cloud computing use has expanded quickly in the two enterprises and in look into. As of late as the information develops quickly, keeping in mind the end goal to meet the business needs combined cloud is embraced. In combined cloud, as the information is put away and handled far from the client and the cloud specialist co-op, protection and honesty of the information assumes a vital part. **Anitha R et al. [14]** proposes a handy and effective strategy for giving security to the information put away at the unified cloud condition utilizing homomorphic strategies. This strategy gives security by putting away the scrambled information in the cloud. The figure key which is produced for scrambling the information assumes a noteworthy part. Authors investigate vital angles inside this specific situation and looks at the part of metadata in information security which enhances the execution in a secured way. The proposed novel homomorphic based key dissemination convention is the key zone under core interest. This proposed work intends to advance the utilization of homomorphism in multi-mists because of its capacity to lessen

security dangers utilizing the upgraded altered feistel procedure.

Distributed computing is a developing system developing quickly step by step because of its minimal effort, unwavering quality and less equipment use. However the possibility of outsourcing an undeniably measure of information and calculation raises different security and protection concern. In this paper **Sweta Agrawal et al. [15]** manage the cryptographic method which depends on Homomorphic Encryption that permits calculation on encoded information other than giving security. Authors attempt to execute Homomorphic Encryption in medicinal area application and checked its security suggestions. However wastefulness in its calculation and CPU use brings constraint for its viable utilize.

IV. CONCLUSION

The data storage service is the fundamental services gave by the cloud provider. The Cryptographic procedures have been utilized broadly in cloud environment. Cryptography is a basic tool that guarantees this information precision. Cryptographic strategies has been adequately lead by the advancement of distributed computing and furthermore because of huge addition in the scope of clients of the cloud. In this review paper, we explored the issue of information security in cloud storage service and its necessity for homomorphic encryption plans. We trust that information stockpiling security in distributed computing is a range brimming with challenges and of fundamental significance. Along these lines the information can be safely imparted to the approved clients by embracing the cryptographic methods.

REFERENCES

[1] ElhamAbd Al Latif Al Badawi and Ahmed Kayed, “Survey on Enhancing the Data Security of the Cloud Computing Environment by Using Data Segregation Technique”, International Journal of Recent Research and Applied Studies, Volume 23, Issue 2, May 2015

[2] RizwanaShaikha and Dr. M. Sasikumar, “Data Classification for achieving Security in cloud computing”, Procedia Computer Science 45 (2015), pp. 493 – 498.

[3] Moritz Borgmann and Tobias Hahn, “On the Security of Cloud Storage Services”, SIT Technical Reports, March 2012

[4] Zeng, W., Zhao, Y., Ou, K. and Song, W., Research on cloud storage architecture and key technologies. In Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, ACM, 2009, November, pp. 1044-1048

[5] SajjadHashemi, “Cloud Computing Technology: Security and Trust Challenges”, International Journal of Security, Privacy and Trust Management (IJSPTM) Volume 2, No 5, October 2013.

[6] Sultan Aldossary and William Allen, “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

[7] Issa M. Khalil and Abdallah Khreishah, “Cloud Computing Security: A Survey”, Computers 2014

[8] Nate Lord, “Cryptography in the Cloud: Securing Cloud Data with Encryption”, Thursday July 27, 2017, available online at: https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption

[9] Kamara, Seny, and Kristin E. Lauter, "Cryptographic Cloud Storage", In Financial Cryptography Workshops, vol. 6054, pp. 136-149. 2010.

[10] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Information Science, 258 (2014) pp. 371-386.

[11] Kamal Benzekki and Kamal Benzekki, “A Secure Cloud Computing Architecture Using Homomorphic Encryption”, (IJACSA) International Journal of Advanced Computer Science and Applications, Volume 7, No. 2, 2016

[12] Maha TEBAA, Saïd EL HAJJI, “Homomorphic Encryption Applied to the Cloud Computing Security”, Proceedings of the World Congress on Engineering 2012 Volume: I WCE 2012, July 4 - 6, 2012, London, U.K.

[13] R. Sharmila, “Secure Retrieval of Files Using Homomorphic Encryption for Cloud Computing”, International Journal of Research in Engineering and Technology, Volume: 03, Special Issue: 07, May-2014.

[14] Anitha R. and Vijayakumar V, “Homomorphic Encryption Based Data Security on Federated Cloud Computing”, ARPN Journal of Engineering and Applied Sciences, Volume 10, No. 5, March 2015

[15] Sweta Agrawal and AakankshaChoubey, “Securing Personalized Medical Data in Cloud Using Homomorphic Encryption”, International Journal of Computer Science Trends and Technology (IJCST), Volume 2 Issue 5, Sep-Oct 2014.