RESEARCHERID
THOMSON REUTERS

[Sridevi * *et al.*, 6(7): July, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON CRYPTOGRAPHIC CLOUD STORAGE TECHNIQUES

Dr. R. Sridevi[*1] & C. B. Banupriya[2]

[*1]Assistant Professor in Computer Science, PSG College of Arts & Science, Coimbatore, India
[2]M.Phil Research Scholar in Computer Science, PSG College of arts & science, Coimbatore, India

DOI: 10.5281/zenodo.829787

ABSTRACT

The cloud computing has become a revolution in information technology, it includes elements from grid computing, utility computing and autonomic computing into a creative deployment architecture. The web service use web service to provide high performance and easy access of storage infrastructure.In this paper a survey of existing cryptographic storage techniques and benefits in cloud computing is discussed

KEYWORDS: cryptographic cloud architecture, cloud computing and storage.

I. INTRODUCTION

The rise in network technology pushes many organizations to outsource their storage.cloud computing is the one where the computer services are available over the internet where the user can access the resources available without having a complete control on them. It encomposes many services such as Infrastructure service (Iaas) where the customer make use of customer services. Platform as a service where the customer leverages the provider resources. Software as a service (Saas) where customer uses software on provider's architecture. Data security, backup, network traffic, file system are the security issues related to cloud.

Cryptography is the art of keeping message secure by changing the data into non-readable forms, Cryptography consists of three algorithms, Symmetric-key algorithms, Asymmetric-key algorithms and Hashing. Crypto cloud is considered a new framework for cyber resource sharing. It protects data security and privacy.It guarantees information security. Security management of cloud computing can also be performed by authorizing the signatures of every element involved. It resolves the conflict service data sharing and privacy security.

This paper is organized as follows. Section II deals with cloud storage, section III describes the security services of cloud. Secton IV deals with the architecture of cryptographic storage. In Section V cryptographic benefits is discuused.

II. STORAGE ON CLOUD

Cloud storage is a service which maintains, manages, and backups the data remotely. Public cloud storage allows customers to move data to cloud instead of using private data storage infrastructure. It provides storage reliablity and availability at a low cost.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

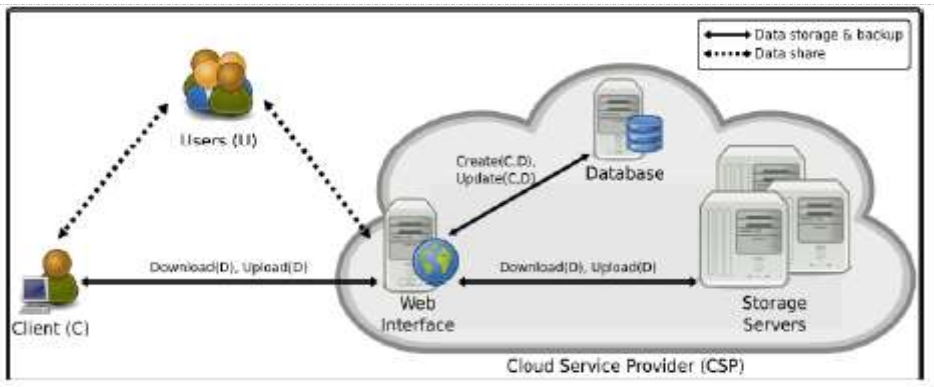

Figure 1 describes the architecture of cloud storage. It depends on following entities.

- Cloud service provider (CSP) manages the distributed cloud storage server and database servers.
- Client can benefit from provider resources and make use of them to share data.
- Users on the other hand are permitted to access the data in cloud based on the authorization provided.

III. SECURITY SERVICES OF CLOUD

When data is stored by the third party the security become a biggest issue. Availability, Integrity and confidentiality serve as the three properties of security. These three properties play an important role in the cloud architecture.

1) **Confidentiality***:* It refers to the authorized parties accessing protected data.Outsourcing data, moving its control to a cloud provider and making it accessible to different parties increase the risk of data breach. A number of concerns emerge regarding the issues of application security and privacy.Multi-tenancy is an important one. It means the cloud characteristic of resource sharing.The cloud computing architecture consists of different kinds of shared resources to enable multiple clients to use the same resource at the same time which presents a number of privacy and confidentiality threats and leads to deadlock.
2) **Integrity***:* It is a process of protecting data from unauthorized deletion and modification of data. The absence of any modification in data between the two updates of data records indicates the consistency of the stored data. Authorization is the mechanism used by the system to determine upto what level authenticated user should have to secure resources.It is important to enforce data integrity.
3) **Availability**: It is a term used by storage service providers (SSPs) to describe products and services which ensure that data continues to be available at a required level of performance in all situations. To ensure availability, the system should be able to operate in all circumstances.

IV. ARCHITECTURE OF CRYPTOGRAPHIC STORAGE SERVICES

The architecture of cryptographic storage consist of three components: a data processor (DP) which processes data before it send to cloud.data verifier (DV) verifies the data in cloud.Token generator (TG) that enable cloud storage provider to retrieve customer data.The researchers proposed many architecture for cryptographic cloud storage some of them are as follows.

Consumer Architecture

Consider three parties- user Alice that stores her data in the cloud; a user Bob with whom Alice wants to share data, and a cloud storage provider that stores Alice's data. To use the service, Alice and Bobby begin by downloading a client application that consists of a data processor, a data verifier and a token generator. During first execution, Alice's application generates a cryptographic key .consider this key as a master key and assume it is stored locally on Alice's system and that it is kept secret from the cloud storage provider. Whenever Alice wishes to upload data to the cloud, the data processor is invoked. It attaches some metadata and encrypts and encodes the data and metadata with a variety of cryptographic primitives. Data sharing between Alice and Bobby proceeds in a similar fashion. Whenever she wishes to share data with Bobby, the token generator is invoked to create a token and a decryption key, which are sent to Bob. He then sends the token to the provider who uses it to retrieve and return the appropriate encrypted documents.Bob then uses the decryption key to recover the files.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Enterprise Architecture

In the enterprise architecture consider an enterprise MegaCorp that stores its data in the cloud; a business partner PartnerCorp with whom MegaCorp wants to share data; and a cloud storage provider that stores MegaCorp's data. To handle enterprise customers, introduce an extra component: a credential generator. The credential generator implements an access control policy by issuing credentials to parties inside and outside MegaCorp. To use the service, MegaCorp deploys dedicated machines within its network.Depending on the particular architecture these dedicated machines will run various core components. Since these components make use of a master secret key, it is important that they be adequately protected and, in particular, that the master key be kept secret from the cloud storage provider and PartnerCorp. If this is too costly in terms of resources or expertise management of the dedicated machines (or specific components) can alternatively be outsourced to a trusted entity. Whenever a MegaCorp employee generates data that needs to be stored in the cloud, it sends the data together with an associated decryption policy to the dedicated machine for processing. The decryption policy specifies the type of credentials necessary to decrypt the data. To retrieve data from the cloud, an employee requests an appropriate token from the dedicated machine .The employee then sends the token to the cloud provider who uses it to find and return the appropriate encrypted files which the employee decrypts using his credentials.

Elliptic Curve Cryptography

The elliptic curve cryptosystem is coined by Koblitz and then Miller in 1985 to design public key Crypto system. It has become an integral part of the modern cryptography. The security intensity of ECC depends on the difficulty of solving elliptic Curve logarithm problem (ECDLP) and it provides the same level of security that is obtained from RSA with less key size .The key strength is the important factor. Elliptic curve is applicable not only in cryptography but also involved in prime test and large integer factorization.It is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

V. BENEFITS OF CRYPTOGRAPHIC STORAGE

The properties of a cryptographic storage service are that control of the data is maintained by the client and the properties of security are derived from cryptography.

- **Regulatory compliance:** In a cryptographic storage service,the data is encrypted on-premise by the data processors.Because of this clients can be assured that the confidentiality of their data is preserved irrespective of the actions done by cloud storage provider. This greatly reduces any legal exposure for both the client and the supplier.

- **Geographic restrictions:** In a cryptographic storage service data is only stored in encrypted form so anything that pertains stored data has no effect on the client. This reduces exposure for the client and allows the cloud storage provider to make maximum use of its storage infrastructure, by reducing its cost.

- **Electronic discovery:** Digital information plays an important role in legal proceedings and often organizations are required to preserve records for data security.

- **Data retention and destruction:** A cryptographic storage service alleviates these concerns since data integrity can be verified and since the information necessary to decrypt data (i.e., the master key) is kept on-premise.

- **Reducing risk of security breaches**: Using cryptographic storage service data in encrypted and data integrity is guaranteed every time. Therefore, a security breach eliminates the risk from the client.

VI. CONCLUSION

The security has became the major issue and challenge in cloud computing, to address this issue many different approaches and models have been proposed by many researchers.cloud service providers are looking for proper techniques to achieve security. This paper provides the survey the cryptographic storage technology in cloud as well as the benefits of cryptographic storage..

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

VII. REFERENCES

[1] Mahima, Yudhveer, " SECURE CLOUD STORAGE ",International Journal of Computer Science & Communication Networks,Vol 1(2), 171-175

[2] Hassan Takabi, James B.D. Joshi, Gail Joon Ahn, "Cloud Computing Security and Privacy Challenges in Cloud Computing Environments ", copublished by the ieee computer and reliability societies,1540-7993/10© 2010 ieee.

[3] Seny Kamara,, Kristin Lauter, "Cryptographic Cloud Storage", Financial Cryptography and Data Security Volume 6054 ,2010, pp 136-149.

[4] G. Ateniese, S. Kamara, and J. Katz. Proofs of storage from homomorphic identi_cation protocols. In Advances in Cryptology - ASIACRYPT '09, volume 5912 of Lecture Notes in Computer Science, pages 319{333. Springer, 2012}.

[5] Yogeswararao Gairaboina1, Y. Siva Prasad2, " A Trusted Cryptography Key Framework for User Data Storage in Cloud Environment", International Journal of Science and Research (IJSR) ISSN (Online): 2319- 7064 (2012)

[6] D. Zissis and D. Lekkas. "Addressing cloud computing security issues". Future Generation Computer Systems, 28(3), 2012, pp. 583-592.

[7] Vishwa gupta, " Advance cryptography algorithm for improving data security ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[8] R. Arokia Paul Rajan, S. Shanmugapriyaa, "Evolution of Cloud Storage as Cloud Computing Infrastructure Service", IOSR Journal of Computer Engineering (IOSRJCE) ISSN : 2278-0661 Volume 1, Issue 1 (May-June 2012), PP 38-45.

[9] Kamara and Lauter: A Searchable, "cryptographic Cloud Storage System", International Scholarly and Scientific Research & Innovation 7(8) 2013.

[10] Rohit S. Bhore, Sejal B. Bharkhada, Ashwini N. Malik, Prof. Anuja K Pande, " Cryptographic Cloud Storage & Networking ", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 12, December 2013 ISSN: 2277 128X Available online at: www.ijarcsse.com.

[11] Rashmi Nigoti1, Manoj Jhuria2 Dr.Shailendra Singh3, " A Survey of Cryptographic Algorithms for Cloud Computing ", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) Available online at: www.iasir.net.

[12] Pratibha Tripathi, Mohammad Suaib#, "Security Issues On Cloud Computing", International Journal of Engineering Technology, Management and Applied Sciences, November 2014, Volume 2 Issue 6.

CITE AN ARTICLE

Sridevi, R., Dr, and C. B. Banupriya. "A SURVEY ON CRYPTOGRAPHIC CLOUD STORAGE TECHNIQUES." *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY* 6.7 (2017): 602-05. Web. 15 July 2017.