A Survey of Cryptographic Hash Function (SHA) in Cloud Storage

Dr. C D Guruprakash[#1], Mr. Subhash C S[#2]

[#1]Professor, [#2] P G Student & Department of CSE & SSIT
Tumkuru, Karnataka, India

Abstract *— The cloud computing has become phenomena its consider to be revolution in information technology, the cloud encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture, Cloud computing offering easy access and high performance computing and storage infrastructure using web service. This rapid movement towards the clouds has impact in level of security the real interesting question is how to build secure cloud storage where service provider is not completely trust customer. In this paper a comprehensive survey of existing literature for cryptographic storage techniques, benefits and drawbacks in cloud computing is presented.*

Keywords — *cloud computing, cloud storage, cryptographic storage architecture***.**

I. INTRODUCTION

The rise in networking technology and the need for computing resources have prompted many organizations to outsource their storage [23]. Cloud computing is the availability of computing services over the Internet where user can use the resource available on cloud without having a complete control on them [24,19]. The cloud computing encompasses many service such as infrastructure service (IaaS) where the customer makes use of service providers computing, network or storage infrastructure, Platform as Service (PaaS) where a customer leverages the provider's resources to run custom applications and finally Software as Service (SaaS) where, customers use software that is run on the provider‟s infrastructure[8,9,10]. Researchers in [25, 9] stated that ensuring data security and privacy in cloud environments is crucial and even of legal concerns. Security issues in cloud computing include data security, backup, network traffic, file system and security of host [17].

Cryptography is the art of keeping message secure by changing the data into non-readable forms, cryptography consist of three algorithms, Symmetric-key algorithms, Asymmetric-key algorithms and Hashing [18]. The real appeal of Crypto cloud computing is that the Crypto cloud is considered a new framework for cyber resource sharing. It protects data security and privacy. In cloud environment, crypto cloud computing guarantees the information security and integrity during the whole procedure. Security management of cloud computing can also be performed by authorizing the signatures of every element involved. What's more, a user can retrieve all related resources by using his QDK key. There is no personal privacy under the current cloud framework [16, 12]. Meanwhile, with the development of crypto cloud computing, we can resolve the conflict between services data sharing and privacy security. It opens up new prospects for the development of information sharing technology [15].

The rest of this paper is organized as follows: Section II introduces cloud storage. Section III describes security service. In section IV Architecture of a cryptographic storage service is presented. In section V an overview of the benefits of cryptography is given. In section VI drawbacks and weakness of cryptography are mentioned. Section VII concludes the paper.

II. CLOUD STORAGE

Cloud storage is a service where data is remotely maintained, managed, and backed up. Public clouds Storage services such as Microsoft's Azure and Amazon's S3 allow customers to shift their data to the cloud by avoiding the costs of building and maintaining a private storage infrastructure. Instead they pay a service provider as a function of its needs. This provides several benefits such as the availability and reliability at a relatively low cost [11, 17].

Fig 1 describes network architecture for cloud storage. It depends on the following entities [7].

1) Cloud Service Provider (CSP) A CSP managed the distributed cloud storage servers and database servers on the resources and allow virtual infrastructure to host application.

2) Client can benefit from providers resources and make use of it to store, retrieve and share his data.

3) Users are permitted to access the content stored in the cloud based on their authorizations provided by the client, these authorize include read write or e-store modified data.

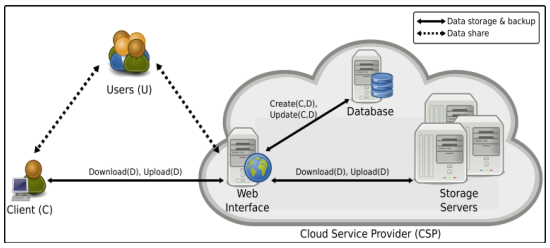

Fig 1. Cloud Storage Architecture

III. CLOUD SECURITY SERVICES

When data is store by using the third party the security issue become more challenging and conflicting [7]. The properties of security are Availability, Integrity and Confidentiality. These three properties have become the key concept used in designing secure systems, especially, in the case of cloud computing architecture [20].

A. Confidentiality: It refers only to the authorized parties or systems that allow accessing protected data [21]. Outsourcing data, delegating 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 multi-tenancy, data remanence, application security and privacy [17]. Multi-tenancy means the cloud characteristic of resource sharing [18]. 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.

B. Integrity: It is a process of protecting data from unauthorized deletion, modification or fabrication. The absence of any alteration in data between the two updates of data records indicating the accuracy and consistency of the stored data, [21]. Authorization is the mechanism used by the system to determine what level of access a particular authenticated user should have to secure resources [37]. According to the rise of the number of parties involved in a cloud environment, authorization is important to enforce data integrity.

***C. Availability*:** It is a term used by computer storage manufacturers and storage service providers (SSPs) to describe products and services which ensure that data continues to be available at a required level of performance in situations ranging from normal to disastrous. System availability includes a system‟s ability to carry on operations even when some authorities misbehave [19]. To ensure availability, the system should be able to operate even if there is a security threat. The user of a cloud environment, who is discharged of hardware infrastructure requirements, relies on the availability of the ubiquitous network.

IV. ARCHITECTURE OF CRYPTOGRAPHIC STORAGE SERVICES

The architecture of cryptography storage consists of three components: a data processor (DP) that processes data before it is sent to the cloud; a data verifier (DV), that guarantee whether the data in the cloud has been tampered with; and a token generator (TG) which generates tokens that enable the cloud storage provider to retrieve segments of customer data. The researchers proposed many architectures for cryptographic storage service in cloud computing below are some of them:

A. Cryptographic cloud storage: The architecture of cryptography storage consists of three components: a data processor (DP) that processes data before it is sent to the cloud; a data verifier (DV), that guarantee whether the data in the cloud has been tampered with; and a token generator (TG) which generates tokens that enable the cloud storage provider to retrieve segments of customer data. The researchers proposed many architectures for cryptographic storage service in cloud computing below are some of them:

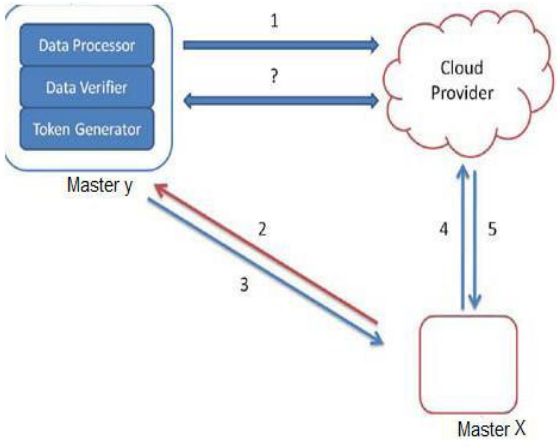

Fig 2. Cryptographic Cloud Storage Architecture

This model includes three substantial stages, which are:

1) Data Processor (DP) that processes data before sending it to the cloud.

2) Data Verifier (DV) which ensure data's integrity.
3) Token Generator (TG) which generates tokens by allowing the service provider to retrieve documents.

B. Associate degree Enterprise architectures: To start Mega corps and partner Corp, the user receives a credential from credential generator. These credentials shall represent information about the user, Mega Corp generates data, and this data needs to be store in the cloud. This data and decryption rule sent to the dedicated machine for processing. In order to retrieve data from cloud, the user requests tokens from dedicated machine. At any time Mega Corp would verify integrity of data, the dedicated machines data verifier is invoked. The next use of the master secret key interacts with storage provider and ascertain data integrity. Here they mention the case when partner corps wishes to access to Mega Corps data the user authenticates itself to Mega Corps dedicated machine and sends its key words then next verified, the certain search is allowed for this partner Crop and dedicated machine sent token in which user used to encrypted files from the service provider, latter it use its credentials to decrypt the file this process is illustrated in fig 3. [12,13].

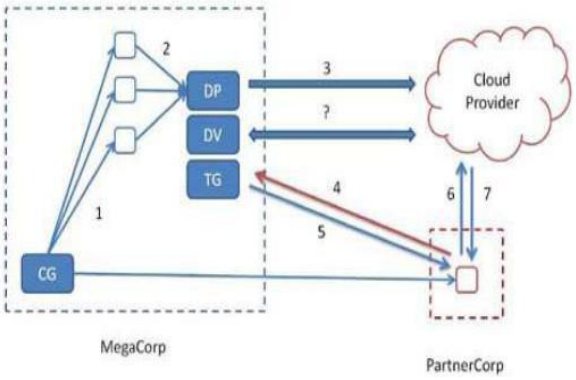

Fig 3. Decipher the File

C. Elliptic Curve Cryptography (ECC): The elliptic curve cryptosystem is coined by Koblitz [6] and then Miller in 1985 to design public key Crypto system. Nowadays, 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 [5]. The key strength is the important factor. Elliptic curve is applicable not only in cryptography but also its involved in prime test and large integer factorization. Combine the true prime test with elliptic curve to develop good primarily test on windows platform [13].

D. DJSA symmetric key algorithm: The researchers in [11] proposed a symmetric key method which used a random key generator for generating the initial key. This key is used to encrypt the source file. The main ideas in this method is to taking four characters from any input file and then search the corresponding file character randomly. After getting the encrypted message, the encrypted data is stored in another file and MSA algorithm is used for searching random key matrix.

E. Homomorphic Encryption: Homomorphic encryption allows processing encrypted data on remote storage without decrypting it, this is a very important method especially when it is used for cloud. Homomrphic encryption verifies the data confidentiality in which it is considered main security issue in case of storage or processing data by an untrusted third party, in fact the owner delegate processing without the ability to access [20] F- RSA algorithm and cloud computing.

RSA is considered the most popular and powerful and secure algorithm nowadays and it's useful for networking security. RSA algorithm along with digital signature is applied for providing cloud data security [13]. Digital signature is used for demonstrating the authenticity of document by applying mathematical schema. In case a receiver receive a valid digital signature it's gave the reason to believe the recipient message is send by known sender and the message is not altered. Digital signature is produced by applying encryption software [14]. Finally, the outcome of this process is called digital signature at the end applying RSA algorithm on that and send "cipher text" at receiver side by using RSA private key decrypt the message and public key is used for signature verification [17]. Cloud service and user interacting by using software interface or API [23].

V. BENEFITS OF CRYPTOGRAPHIC STORAGE

Cryptography in cloud computing gives many benefits such as:

A. ***Confidential Assurance:*** In a crypto logical storage service, the data is encrypted on-premise by the information processor(s). In this way, the customers will be protected and enforcing confidentiality of their knowledge is preserved, irrespective of the actions of the cloud storage supplier. This greatly reduces any legal exposure for every client and supplier [20].

B. ***Geographic restrictions:*** In a crypto logical storage service, knowledge is barely stored in an encrypted kind, any law that so pertains to the keep knowledge has very little or no impact on the customer. This is really a less legal exposure for the customer and allows the cloud storage supplier to make optimum use of its storage infrastructure, thereby reducing prices [1, 2].

C. ***Subpoenas:*** In a crypto logical storage service, since knowledge is stored in an encrypted kind and since the client retains possession of all the keys, any request for the (unencrypted) knowledge should be created on to the customer [14].

D. ***Reducing Risk of Security Breaches:*** Even if a cloud storage supplier implements sturdy security practices, there's always the likelihood of a security breach. In this situation the client might be legitimate accountable. Using cryptographic storage service data in encrypted and data integrity is guarantee at any time. Therefore, a security breach poses very little and eliminates the risk from the client. [21]

E. ***Data Retention and destruction:*** In many situations, a client has the responsibility for retention and destruction of data it has collected while this data is bean store in could it may be hard to the customer to ascertain the data integrity and ensure whether it was properly discarded. A crypto logical storage service alleviates these issues since knowledge integrity will be verified and since the knowledge necessary to decipher knowledge (i.e., the master key) is kept On-premise. Secure knowledge erasure will be effectively achieved by simply erasing the master data [24].

F. ***Electronic discovery:*** Using cryptographic storage service will verify integrity at any point if a provider has incentive to preserve the Data integrity [12].

VI. CONCLUSION

The common issue and challenge for cloud computing is the security of the cloud environment, many different approaches and models have already been proposed by many researchers. Cloud services providers are now searching for the proper security and privacy mechanisms which would make the cloud atmosphere safe and protected place for their customers and they keep full faith on the cloud service provider. This paper survey the cryptographic storage technology in cloud computing the techniques.

REFERENCES

[1] Sandip S. Dabre1 , Mangesh S. Shegokar2, " Mechanism for secure Big data stored within cloud storage by using cloud computing (Secure cloud storage)" , International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 4 April 2015, Page No. 11306-11309

[2] Mahima, Yudhveer, " Secure Cloud Storage ",International Journal of Computer Science & Communication Networks,Vol 1(2), 171-175 [3] Kamara and Lauter: A Searchable, "ryptographic Cloud Storage System", International Scholarly and Scientific Research & Innovation 7(8) 2013.

[3] Luan, Shang-Wen, et al. "Development of a smart power meter for AMI based on ZigBee communication", Power Electronics and Drive Systems, 2009. PEDS 2009. International Conference on. IEEE, 2009.

[4] G. Ateniese, S. Kamara, and J. Katz. “Proofs of storage from homomorphic identification 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 Impact Factor (2012): 3.358

[6] Alowolodu O.D, Alese B.K, " Elliptic Curve Cryptography for Securing Cloud Computing Applications " , International Journal of Computer Applications (0975 – 8887) Volume 66– No.23, March 2013

[7] Nesrine K aaniche , Aymen Boudguiga, Maryline aurent, " ID -Based Cryptography for Secure Cloud Data Storage", IEEE sixth international conference 2013 Page(s):375 - 382

[8] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, [online]. http://www.theregister.co.uk/

[9] 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/$26.00 © 2010 IEEE.

[10] Australian government department of defense, "Cloud Computing Security Considerations", Cyber Security Operations Centre April 2011, Updated September 2012.

[11] Seny Kamara, " Cryptographic Cloud storage", proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010 [12] 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

[12] The Cointelegraph, A Brief History of Ethereum From Vitalik
[13] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. Skeith. “Publickey encryption that allows PIR queries”, In A. Menezes, editor, Advances in Cryptology - CRYPTO '07, volume 4622 of Lecture Notes in Computer Science, pages 50-67. Springer, 2007.
[14] Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari, "Security on Cloud Using Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015 ISSN: 2277 128X Available online at: www.ijarcsse.com
[15] Jean-Jacques Quisquater, How to Explain Zero-Knowledge Protocols to Your Children, 1989.
[16] Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari, "SecurityonCloudUsingCryptography",InternationalJournal ofAdvancedResearchinComputerScienceandSoftwareEngineering,Volume5,Issue3,March2015ISSN:2277128XAvailableonlineat:www.ijarcsse.com
[17] JamesMark Kelly, Columbusstate University CPSC 6128 Spring 2010-Cloud computing and cryptography
[18] Neha Jainand Gurpreet Kaur „”Implementing DES algorithmin Cloud for Data Security” VSRD.
[19] 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
[20] G. Murugaboopathi, C.Chandravathy, P. Vinoth Kumar, " Study on Cloud Computing and Security Approaches", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013
[21] Sana Belguith, Abderrazak Jemai, Rabah Attia, " Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm ", ICAS 2015 : The Eleventh International Conference on Autonomic and Autonomous Systems.
[22] Evan Duffield,Daniel Diaz ,Dash: “A Privacy-Centric Crypto-Currency”, 2015.
[23] D. Zissis and D. Lekkas. “Addressing cloud computing security issues”. Future Generation Computer Systems, 28(3), 2012, pp. 583-592 [22]Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010
[24] Seny Kamara,, Kristin Lauter, "Cryptographic Cloud Storage", Financial Cryptography and Data Security “ Volume 6054 ,2010, pp 136-149
[25] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”. In Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW ″09, pages 85–90, New York, NY, USA, 2009. ACM