SURVEY: DATA INTEGRITY AND SECURE STORAGE OVER CLOUD

Akansha Shrivasava
School Of Information Technology
UIT, RGPV
Bhopal, M.P. India
e-mail address if desired

Dr. Varsha Sharma
School Of Information Technology
UIT, RGPV
Bhopal, M.P. India
e-mail address if desired

Abstract*—Data storage and its integrity monitoring is a high level task in cloud computing platform, where multiple files with heavy size are stored and further there is chance to find attack from different entities. In the scenario where the security check-up is not possible manually, integrity verification technique works where the data can be break into blocks and then further blocks can get security and further a integrity verification can be perform using hashing algorithm. In this paper our objective is to survey such techniques which claims as the best security and integrity checksum level technique to provide data security assured. The paper further investigated the drawback of various existing technique in this field.

***Keywords*—Cloud data integrity, cost reduction, hashing scheme, Cloud data storage**

I. INTRODUCTION

Cloud computing, also known as 'on-demand computing', is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort.

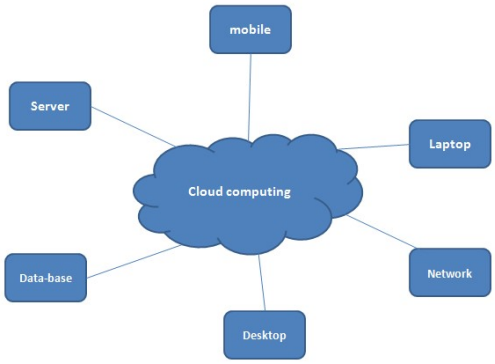

Figure 1 : Cloud Computing

A description of the cloud is presented in Figure 1, in that there are various user which uses various devices like Mobile, desktop, Laptop, server etc. are connected Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing Security:

Cloud computing security [3] or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing**.** A user data stored at cloud server and user concern about the security of that data.

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. [4] The security management addresses

these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack.

Rest of the paper organizes as follows:

II Literature Review, a brief literature review over the various techniques is presented, III conclusion.

II. LITERATURE REVIEW

Satheesh K S V A Kavuri, Dr.Gangadhara Rao Kancherla, Dr.Basaveswara Rao Bobba, 2014,

In this paper a study is discussed on the previous hashing and data verification technique which were given based on file size and other property. In order to overcome these limitation author proposed a work where a ABE technique is performed, also they used 512 bit size of hash value which is stored in cloud. They proposed an authorization technique with cloud computing to use remote files. They proposed a DUPHA a hashing algorithm which produce hash from the data and further an IAB encryption model is performed. Using this approach a proper authentication of data in different user is performed. They have also used a proper partitioned algorithm for the data where the different copy can generate and store over the cloud. 10 rounds of approach is used for 512 bit key data generation process. Finally they have implemented the algorithm using Java Swing API platform and they performed encryption and hashing via DUPHA approach. Finally they have compared with whirlpool algorithm with parameter of hashing access time in ms [1].

Dr. M. Srivenkatesh, Ms.K.Vanitha, 2015,

In this paper a cryptographic hash function is used in order to produce a high dimension secure data for the cloud server. A Modern MD5 hashing algorithm which puts 32 bit size of block data and keep generate hashing value using this MD5 technique. The federated cloud computing environment is used by the party to execute the scenario. Finally in order to implement encryption model public key cryptography for maintaining the privacy of data in the federated cloud computing. The limitation of the system can be found as the low data hashing size as compare to SHA technique available today [2].

Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, and Martin Sch, and Yu Sasaki, 2011

In this paper a whirlpool mechanism for hash generation is used where a 512 bit block of data is used. In this algorithm they use file size, file metadata information is used where these property taken as input and generate as output data to upload on cloud server. This algorithm is not belongs to MD-X group and it operate on the mechanism of AES algorithm. It is good alternative to use to ensure algorithm diversity. Previously it has 6 rounds to generate the hash and then further extends to 8 round while working with hashing generation. In order to avoid collision this algorithm prompts as best algorithm to get hashing generation. A limitation to this algorithm is data is not base for hash generation, it takes the metadata property for hashing generation which is not correct sometime [5] [6].

Miss. M.Sowparnika, Prof. R. Dheenadayalu, 2013

Here in this paper an approach is used for the hashing generation where association rule algorithm is used as hyper edges. A module from the TPA, cloud server and storage is used in order to perform security model with this approach. They have utilized an RSA algorithm for the encryption system and also a batch auditing concept is driven by them to provide a cloud server approach for secure authentication and storage. They have also stated the advantage of their proposed mechanism as user can assure that all data in cloud are in protected condition for its trustworthiness. So the actual size of stored data in cloud is easily maintain even though the user himself has done any modification, deletion and update for his purpose by using proposed scheme. A homomorphism authenticator is used to make data privacy preserving from the different number of users [7].

Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo and Xiaofen Wang,2015

In this paper a new dual server public key encryption technique is presented. In that technique a new variant of SPHF (Smooth Projective Hash Function) is used. In that Linear and homomorphic SPHF is presented, which provide an enhanced functionality to provide secure storage for the data in cloud storage. In cloud data resides at cloud server which is vulnerable to various attacks like key guessing attack etc. Thus that technique not provides enhanced functionality to restrict such attacks in cloud storage.

Sheren A. E-Booz, Gama, Attiya and Nawa, E-Fishawy, 2015

An enhanced framework for secure cloud storage system is presented by the authors. This system protects data from both

cloud service provider and third party auditor. In cloud computing user's data resides in cloud server, which is vulnerable for various attacks. Generally third party auditor (TPA) is used for that purpose to take care about all the security concern of that data. But the role of TPA is also suspicious, might be it leaks data, data integrity also lost during that process etc. thus a new technique which provides security from both cloud server and TPA to preserve privacy of the data is presented. In that technique a time based one-time password (TOTP) and automatic blocker protocol is presented to provide better performance in secure cloud storage for the data [13].

Deepnarayan Tiwari and G. R. Gangadharan, 2015

In this paper author described that, in cloud computing user data stored at an outsourced environment which requires an enhanced technique to provide a secure storage framework for that data. In that technique an attribute broadcast encryption, attribute based access control and proxy re-encryption technique can be used to provide an enhanced technique to provide a secure storage for the data in cloud computing. In attribute based encryption attributes of the data are used to encrypt data that enhances security of the data [14].

Fei Chen, Tao Xiang, Yuanyuan Yang, Sherman S. M. Chow, 2014

In this paper a secure cloud storage protocol is presented which supports public verifiability to the protocol. In that technique combination of secure cloud storage protocol and secure network coding is used to provide a secure mechanism to deal with such issues. This technique is also provides advanced functionality to third party public auditing [15].

Third party cloud storage and access permissions play a vital role in security analysis and user access control. User access control and data verification are the important revolutionary technologies to provide security and control unauthorized users. Third party cloud servers are built without proper security measures and user control mechanisms. User can access the data such as documents, media or other type of files using third party generated authentication key and secret information.
Traditional cloud security mechanisms are independent of data integrity verification to the authorized data users. Third party cloud servers are vulnerable to different type of message integrity attacks. Traditional message integrity algorithms are depend on the file size, hash size and security parameters.

C. Selvakumar G. Jeeva Rathanam M.R.Sumalatha, 2013

Each user's data is given input to hash algorithm to calculate 512-bit hash value. In the next process, generated hash value is given input to improved attribute based encryption model for data encryption. Both the encrypted data and its hash value are stored separately in the cloud storage. Similarly, the reverse process can be used to restore the original data through data integrity method proposed system which uses RSA which create public and private RSA key for encrypting the files, and stored in cloud. The generated private key length is 2048 bits [17].

R. Sanchez et al. 2012

In this paper author have discussed about privacy enhanced and trust-aware IdM architectures, that enables to keep to a trace-off between user's privacy and degree of tracking to obtain an adequate personalization degree in the different services. This framework is designed based on the importance of cloud consumers. User information security analysis providing Identity management and authentication is learnt from this paper. Hence an innovative mechanism which provides secured data storage and fault tolerance is handled in the proposed work [19].

Elena Ferrari and Bhavani Thuraisingham, 2012

In this paper author have shown the importance of securing the data using Data and Applications Security and Privacy (DASPY) framework from unauthorized access due to the explosion of sensitive or private data.This work gives insights of how to integrate value-added security characteristics into today's cloud storage services [20].

Ravi Jhawar et al. 2013

In their work proposed handling fault tolerant techniques with a high level approach by designing a separate service layer. Fault tolerance is further strengthened by providing integrated diagnostic approach and isolation of the node recovery mechanisms in the proposed work.Solutions were also provided to have an effective and secured fault tolerant data storage issues by analyzing the data [22].

Technique	Advantages	Disadvantages

DUPHA [1]	Enhanced functionality to provide secure cloud storage, Whirlpool hashing algorithm used with ABE to provide encryption, Better performance to generate hash value for the data	No security for TPA. Whirlpool requires more hardware assistance than the SHA-512, generates Hardware overhead.
Modern MD5 hashing algorithm[2]	Which puts 32 bit size of block data and keep generate hashing value using this MD5 technique	Low data hashing size as compare to SHA technique.
Whirlpool mechanism for hash generation [6]	hash generation is used where a 512 bit block of data is used	data is not base for hash generation, it takes the metadata property for hashing generation which is not correct
Association rule algorithm [7]	A module from the TPA, cloud server and storage is used in order to perform security model is used	cloud server approach for not secure authentication and storage
Smooth Projective Hash Function [12]	Provide an enhanced functionality for secure storage for the data in cloud storage	Not have proper functionality to restrict attacks in cloud storage
TOTP and Automatic Blocker Protocol [13]	Provides a security mechanism, to preserves security of data from TPA and Cloud server both and also protect it from intruders. Time based one-time password, and authentication blockers are used to provide better security for the data.	It uses authentication blocker which is not efficient and time consuming process. Sometimes it also vulnerable for Guessing attacks.
TPA based authentication technique [16]	In that a third party authentication mechanism is used to reduce overhead of the user, and take care of all the auditing tasks.	But the role of TPA, is suspicious data may be leaked, Which compromise integrity and confidentiality of the data.

Table 2.1: Comparison of Various techniques used for integrity and secure cloud storage

III. CONCLUSON

In this paper different approaches and multilevel technique for the cloud data storage and retrieval has been discussed. The multiple researches proposed their hashing technique to data checksum and verifying the data with its integrity level. The recent technique described the approach in which data is divided in block of 512 byte and then processed for hash and encryption. Our further work is going to find a new approach to overcome the drawback driven by the existing approach in same category to make cloud platform stronger. As per the recent work DUPHA performed with ABE encryption given low execution time while performing hashing on different data size. But there are some drawbacks like it requires more hardware consumption than SHA-512 based technique and also not provides security mechanism in third party scenario. Thus an enhanced technique is required to provide better performance to the user to provide a secure cloud storage in cloud computing.

REFERENCES

1. Satheesh K S V A Kavuri, Dr.Gangadhara Rao Kancherla, Dr.Basaveswara Rao Bobba," Data Authentication and Integrity Verification Techniques for Trusted/Untrusted Cloud Servers", 2014 IEEE.
2. Dr.M.Srivenkatesh1,Ms.K.Vanitha2," A Secure Development Scheme of the HashFunction and its Implementation in Public Key Cryptography for Maintaining the Privacy of Data in the Federated Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4,April2015.
3. L. Arockiam S. Monikandan. Efficient Cloud Storage Confidentiality to Ensure Data Security,2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 05, 2014
4. R. Navajothi , S. Jean Adrien Fenelon , An Efficient, Dynamic, Privacy Preserving Public Auditing method on un trusted cloud storage , International Joint Conference of IEEE TrustCom,2014.
5. Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, and Martin Schl. Rebound distinguishers: Results on the full Whirlpool compression function. In Matsui , pages 126{143.
6. Yu Sasaki. Meet-in-the-middle preimage attacks on AES hashing modes and an application to Whirlpool. In Antoine Joux, editor, FSE, volume 6733 of Lecture Notes in Computer Science, Springer, 2011.
7. Miss. M.Sowpamika, Prof. R. Dheenadayalu "Improving data integrity on cloud storage services" International Journal of Engineering Science Invention, Vol. 2, February 2013, pp.49-55.
8. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Cooperative provable data possession" Cryptology ePrint Archive, Report 2010/234, 2010.
9. Hassan T, James B.D. Joshi, et al., "Security and Privacy Challenges in Cloud Computing Environments" IEEE Security and Privacy, vol. 8, pp.24-31, Nov-Dec 2010.
10. Pardeep K, Vivek K.S., et al., "Effective Ways of Secure, Private and Trusted Cloud Computing" International Journal of Computer Science Issues, Vol. 8, May 2011, pp.412-421.
11. Yogeesh A.C,Dilip B.R,Chandra,Divya S Abhyankar "Ensuring Scalable, Secured, Maintenance and Access control of College Data, Using Cloud Computing". International Journal of Advances in Engineering & Technology, May-2012
12. Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo and Xiaofen Wang "Dual-Server Public-Key Encryption with KeywordSearch for Secure Cloud Storage" IEEE, 2015.
13. Sheren A. E!-Booz, Gama! Attiya and Nawa! E!-Fishawy "A Secure Cloud Storage System Combining Time-based One Time Password and Automatic Blocker Protocol" IEEE, 2015.
14. Deepnarayan Tiwari and G. R. Gangadharan "A Novel Secure Cloud Storage ArchitectureCombining Proof of Retrievability and Revocation" IEEE, 2015
15. Fei Chen, Tao Xiang, Yuanyuan Yang, Sherman S. M. Chow "Secure Cloud Storage Meets with Secure Network Coding" IEEE, 2014.
16. ANUPRIYA.A.S, ANANTHI, Dr. S KARTHIK, "TPA based cloud storage security techniques", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 8, October 2012.
17. M. R. Sumalatha , C. Selvakumar , G. Jeeva Rathnam, "Secured Data Storage and Error Tolerant Design in Cloud Computing", 2013 International Conference on Recent Trends in Information Technology (ICRTIT).
18. Dynamic Secure Storage System in Cloud Services. G.JeevaRathanam IEEE Dec2014.
19. Rosa Sanchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sanchez and Andres Marín, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, pp. 95-103, February 2012.
20. Elena Ferrari and Bhavani Thuraisingham, "Guest Editors' Introduction: Special Section on Data and Applications Security and Privacy" IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 5, pp. 625-626, October 2012.
21. Data Authentication and Integrity Verification Techniques for Trusted/Untrusted Cloud Servers, Satheesh K S V A Kavuri, Dr.Gangadhara Rao Kancherla, Dr. Basaveswara Rao Bobba. 2014 International Conference Advances in Computing, Communications and Informatics (ICACCI) IEEE Dec 2014.
22. Ravi Jhawar, Graduate, Vincenzo Piuri and Marco Santambrogio, "Fault Tolerance Management in Cloud Computing:A System-Level Perspective" IEEE Systems Journal, Vol. 7, No. 2, pp. 288-297, June 2013.

