IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Secure Technique to Achieve Data Privacy and Data Integrity in Cloud Computing

Shraddha Saxena[1*], Manish Sharma[2]

[1,2]Dept. of Computer Science, Suresh Gyan Vihar University, Jaipur, India

[*]*Corresponding Author: sxn.shradha17@gmail.com, Tel.: +91-8114462586*

Available online at: www.ijcseonline.org

Accepted: 20/Oct/2018, Published: 31/Oct/2018

***Abstract*—** Cloud services are increasing day by day over the Internet. Using the cloud services both time and money will be saved for user. However, there are some security problems to be solved for users and enterprises for data storing in secure way in the cloud. The real fact is that when users will have not any kind of physical control on outsourced data. Cloud user is concerned about the security and integrity of data stored in the cloud environment as it can be attacked by attacker. The purpose of this research paper using Third Party Auditor an efficient public data auditing technique works for verify the security and integrity of data. Which data is stored in the cloud. The proposed auditing technique makes use of Secure Hash Algorithm (SHA-2) for generating verification meta data and message digest for data integrity authentication and AES algorithm for encryption. Analysis of proposed technique shows provably more secure and TPA takes a constant time to audit files of different sizes.

***Keywords*—**Cloud Computing, Public Auditing, Data Integrity, Data Privacy, Third Party Auditor (TPA).Cloud Service Provider (CSP).

I. INTRODUCTION

Cloud is a computing paradigm in which resources are shared as a service over the internet. Cloud data storage is one of the service provided by Cloud computing in which data is managed, maintained, backed up remotely and made available to users over the internet. Moving data in cloud offers great convenience for users since they don't have to care about the complexities of hardware management[1].
The Cloud Computing vendors, Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) are both well-known examples. These Internet-based on-line services do provide huge amounts of storage space and customizable computing resources. This computing platform eliminates the responsibility of local machines and users can be relieved from the burden of local data storage and maintenance.

There are many benefits of cloud services, users are reluctant to adopt this technology because of security threats [2].There are many threats facing the cloud not only from an outsider but from an insider which can utilize cloud vulnerabilities to do harm. These threats may harm data confidentiality, data availability and data integrity. Some untrusted providers could hide data breaches to save their reputations or free some space by deleting the less used or less accessed data [3]. In sensitive and confidential data, there should be some security mechanism to provide protection for cloud data. To keep away from the security risks, audit services and concept of cryptography are significant to make sure about the confidentiality and integrity of outsourced data. Auditing introduced in Cloud computing to deal with secure data storage.

Research contribution
1. Identifying cloud services for organization like EC2, S3
2. Specifying various techniques used for securing the data of organization or individual user.
3. designed improved technique for securing data with integrity

II. RELATED WORK

Different factors such as data integrity, confidentiality etc. affects the performance of cloud data storage. There has been a lot of development in this field and lots of algorithms have been proposed by various researchers. Here we are presenting the related works that are found to be useful.
TABLE 1 represents the comparison done by considering different factors such as methods used, supports privacy preserving, supports public auditing, data confidentiality and maintaining data integrity

Research Work	Methods Used	Supports Public Auditing	Maintaining Data Integrity	Supports Privacy Preserving	Maintaining Data Confidentiality
Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm[5]	HMAC	Yes	Yes	Yes	No
Privacy Preserving Public Auditing for Secure Cloud Storage[6]	HLA with BLS Signature	Yes	Yes	Yes	No
Privacy Preserving and Public Auditing Service for Data Storage in Cloud Computing [7]	RSA and MHT	Yes	Yes	Yes	Yes
Towards Secure and Dependable Storage Services in Cloud Computing [8]	Homomorphic Tokens and Erasure code	Yes	Yes	Yes	No
Privacy-preserving Public Auditing for Data Storage Security in Cloud Computing [9]	HLA with Random Masking	Yes	Yes	Yes	No
Secure and Efficient Privacy Preserving Public Auditing Scheme for Cloud Storage [10]	HLA with BLS Signature	Yes	Yes	Yes	No

Swapnali proposed a efficient privacy preserving and secure public auditing technique[5]. Using a Third Party Auditor. By this technique user achieves public auditing and privacy preserving for cloud . The owner of data or users are responsible in cloud services for splitting the file into blocks, generating a SHA-2 hash value for each block of file and encrypting data by using AES algorithm, concatenating the hash value and generates a RSA signature. the RSA signature generated by TPA and the one stored in the other Third Party Auditor in the verification process. its provided by the data user and compared by the Third Party Auditor. data is intact when both data matches, and if data mismatch then the data integrity has been tampered or affected.

Tejaswani achieved integrity of data using a Merkle Hash Tree by confidentiality and Third Party Auditor of data is achieved using RSA based cryptographic algorithm[6]. According to table it is clear that different techniques have been developed to check the integrity of the data. But each method has some unique problems. The existing methods succeeded in providing public auditing along with privacy preserving but failed to maintain the confidentiality of data. So its necessary to develop a efficient secure auditing scheme which has to perform the public auditing effectively by maintaining both the confidentiality and integrity of cloud data.

Ezhil has proposed a technique that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to improve the security of Third Party Auditor[7]. This technique used for verifying the authenticity of a data transmitted between two parties that agree on a shared secret key. HMAC's are based on a key that is shared between the two parties, if either party's key is compromised, it will be possible for an attacker to create fraud messages.

Cong proposed a secure cloud data storage system supporting privacy-preserving public auditing[8]. In this technique they utilized random masking technique and the homomorphic linear authenticator to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server. They extend their protocol into a multiuser setting, where the Third party auditor perform many auditing tasks in a batch manner for better efficiency. Even this technique provides public auditing and efficient privacy preserving, it lags in security concern. Less security is provided to data when compared to the systems that used encryption/ decryption algorithms.

III. METHODOLOGY

In this research paper mainly focuses on security issues of cloud data storage[9]. the cloud data storage service involving three different entities. The proposed technique consists of three basic entities, they are cloud user, cloud server and Third Party Auditor.

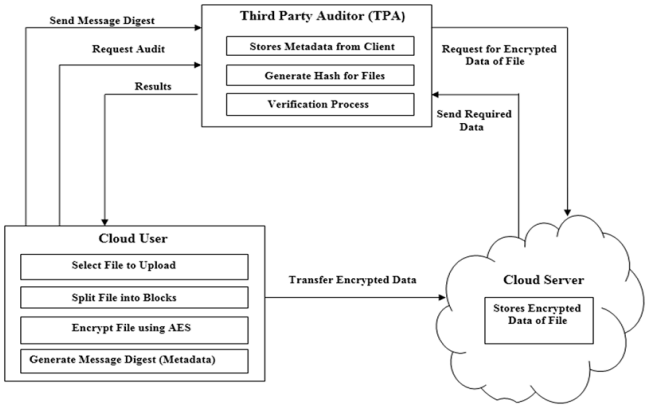

Fig. 1. Architecture of novel Proposed technique

If the data owner authenticates cloud server by providing his password, the data owner selects the file to upload in cloud server and after uploading its splited into blocks. The blocks are encrypted using AES algorithm followed by generating message digest using Secure Hash Algorithm (SHA-2). A copy of encrypted file is transferred to cloud for storage. Later the message digest is sent to Third Party Auditor. Its uses this digest to check the integrity of data stored in the cloud server storage. Since meta data is sent to Third Party Auditor, TPA will not get enough information about users.

TPA performs data auditing according to demand by the client. After receiving the auditing request from cloud data owner or user, the Third party challenges cloud server to send the encrypted data of files that are stored in cloud storage. After getting the encrypted data from cloud server the Third party follows the same process performed by data owner such as generating message digest for encrypted blocks of data using SHA-2 algorithm**.**

The working of the cloud user in our proposed system is illustrated in figure 2 and figure 3.

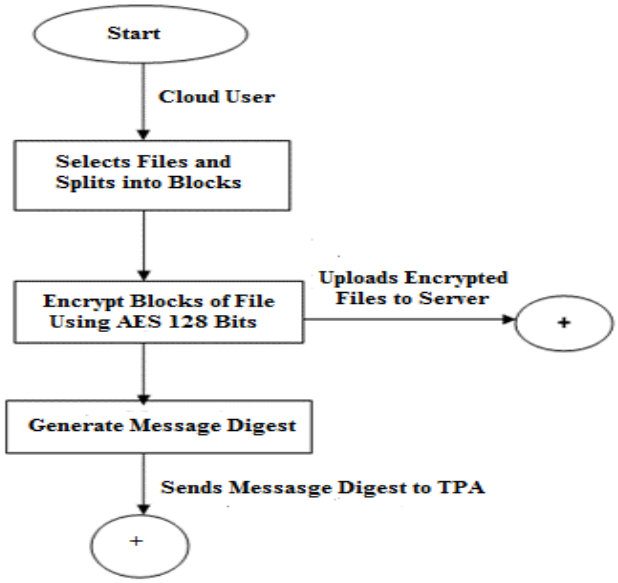

Fig. 2. Work flow of Cloud User

In the verification process, it compares the newly generated message digest value with the earlier message digest sent by client. If both the values are matched then it indicates that the integrity of data is maintained. If there exists a mismatch, indicates that data is altered and integrity is not maintained. Finally the TPA will send auditing results to the data owner indicating the status of file.

The cloud server is used to store the encrypted data of files[10]. When it receives request from the TPA, the cloud server will send required encrypted blocks of data to TPA. In the proposed scheme cloud users can upload files to cloud server and can rely on TPA to check the integrity of data stored in cloud server.

IV. IMPLEMENTATION & RESULT

The proposed technique implemented by python on a system with Intel core i5 processor running at 2.33 GHz and 4GB RAM. HTML5 and CSS3 are used to develop front end. Advanced Encryption Standard (AES 128 bit encryption) algorithm is implemented using python language and it is used for encrypting blocks of data. Secure Hash Algorithm (SHA-256 bit) implemented in python by using Hash-lib module/library. This module implements a common interface to many different hash algorithms and secure message digest.

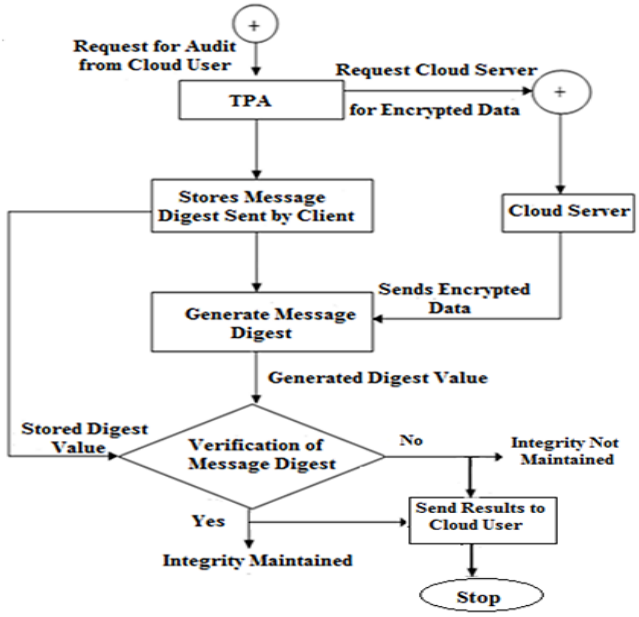

Fig. 3. Working process of TPA

SHA 2 is used to generate verification meta-data or a digest for a given data. It generates an almost-unique 256-bit (32-byte) cryptographic hash or digest for a text. The following

are some of the 32 byte (256 bits) digest we obtained during the analysis of our proposed technique.

1.d3bdb4bb29c8e29be3f64f23d4df4673fd2a2f29c39986933502e8f0465daee3.
2.837c8ab3afaa0d10c1a58902d58d46a41085e036506092134d3fffb97c4507bf.

To achieve constant bandwidth, we took files ranging from 100KB to 1000KB. The figure 4 represents the time taken by TPA to audit the files ranging from 100KB to 1000KB. In our observation, comparing our proposed system with [7], we find in our system will also take constant time to audit the files of different file sizes.

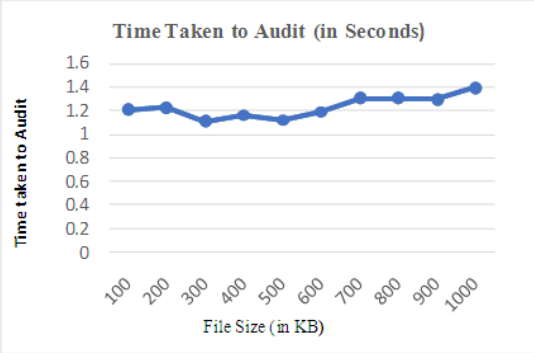

Fig. 4. File Size vs. Auditing Time

V. CONCLUSION A ND FUTURE WORK

In this research paper, we proposed a privacy preserving public auditing technique for data storage security in cloud system. Third party auditor will perform auditing task without retrieving the data of a cloud user, achieves privacy preserving. Before uploading any data in cloud, by this technique the user's data is encrypted first and then stored in the cloud storage in encrypted form, which works for achieving the confidentiality of data. The integrity of data is evaluated by TPA by verifying both the message digest. TPA checks whether the data stored in cloud is tampered or altered and later report the same to the cloud user. All modules in the system are implemented to develop an effective auditing technique.

Current technique work on static data in future want to perform data dynamic operations such as insertion, updation and deletion and of data.

REFERENCES

[1] W. A. Sultan Aldossary, "Data Security, Privacy, Integrity and Availability in Cloud Computing", International Journal of Advanced Computer Science and Applications,Volume 7, Issue 4, pp. 485- 498, 2016.

[2] Amazon.com, "Amazon Web Services (AWS).

[3] X. Jia and N. K. Yang, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities", World Wide Web, Volume 15, Issue 4, pp. 409–428, 2012.

[4]. Cong Wang , Sherman S M Chow, Qian Wang, Kui Ren, and Wen jing Lou. "Privacy Preserving Public Auditing for Secure Cloud Storage." IEEE Transactions on Computers, Volume 62, Issue 2, February 2013.

[5] . Sangita Chaudhari, Swapnali More, , "Third Party Public Auditing Scheme for Cloud Storage", International Journal of Procedia Computer Science, Volume 79, pp. 69-76, 2016.

[6] Tejaswini, K. Sunitha, and S. K. Prashanth. "Privacy Preserving Public Auditing Service for Data Storage in Cloud Computing". Indian Journal of Research PARIPEX, Volume 2, Issue 2, pp. 131-133, February 2013.

[7] S Ezhil Arasu, B Gowri, and S Ananthi. "Privacy Preserving Public Auditing in cloud using HMAC Algorithm". International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277, 3878, Volume 2, Issue 1, pp. 149-152, March 2013.

[8]. Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou. "Towards Secure and Dependable Storage Services in Cloud Computing". IEEE Transactions on Services Computing, Volume 5, Issue 2, pp. 220–232, May 2011.

[9] Wang, C., Wang, Q., Ren, K., Lou, W., 2010. "Privacy-Preserving Public Auditing for Data Security in Cloud Computing". In: INFOCOM, 2010 Proceedings IEEE, pp. 1–9, 2010.

[10]. Solomon GuadieWorku, Jining Zhao, Chunxiang Xu, and Xiaohu."Secure and Efficient Privacy-Preserving Public Auditing Scheme for Cloud Storage". Computers & Electrical Engineering, Volume 40, Issue 5, pp. 1703-1713, July 2014.

Authors Profile

Shraddha Saxena pursed B.tech from Rajasthsn College of Engineering for Women, Jaipur and perusing Master of computer science & Engineering from Suresh Gyan Vihar University, Jaipur. Her main research work focuses on cryptography, web security cloud computing, Network Security, Cloud Security and Privacy, Data Mining and Computational Intelligence based education.

Manish Sharma is Assoiate Professor in Computer Engineering & Information Technology Department, Suresh Gyan Vihar University. He has done his M.Tech. (Computer Science) from Birla Institute of Technology, Mesra, Ranchi in 2000, and M.Sc. in Mathematics from University of Rajasthan, Jaipur in 1992. He is currently working as Director IQAC, Suresh Gyan Vihar University. He has participated and presented many papers in various Conferences and Seminars of National/International repute. He has undertaken various projects like Market Gold (Developed in VB-6 and SQL-Server) in BIPS Info-tech, Jaipur, Stock Gold (Developed in VB-6 and SQL-Server) in BIPS Info-tech, Jaipur, Electricity Billing System in BIPS Info-tech, Jaipur, Computer Integrated Home security System (Developed in C++), Electronic controlling integrated in C language.

