International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Secure Cloud Storage using Secret Key Sharing and Proxy Re-Encryption Based Third Party Auditing Service

Dasari Venkata Ramesh

Abstract*: *Cloud Computing (CC) provides an easy way to access and store the information by vast remote servers, instead of using personal computer. There is no physical control over personal data by user, hence some security issues may arise for users and organization to secure the data in cloud. The sensitive data can be hacked by attackers, so the integrity of data stored in cloud is a major concern for users. In this research work, the data integrity can be ensured by using Third Party Storage Auditing Service (TPSAS), where it satisfies all the requirements of users in cloud. The ultimate aim of this research is to avoid the unauthorized access of user's data stored in the cloud. In this paper, two major problems are considered for attaining the integrity of data in the cloud. The first one is, the unauthorized user tries to modify the data, which is solved by the proposed TPSAS. The second problem considered in this research is, since the Cloud Service Provider (CSP) is semi trustable it can be malfunctioned at any time, which can be solved based on the secure secret key sharing algorithm and proxy re-encryption methodology. The secure secret key sharing is implemented based on the Shamir key sharing algorithm and the proxy re-encryption process is implemented based on the bear and lion proxy re-encryption methodology.

Index Terms*: *Cloud Service Provider, Cloud Storage, Proxy Re-encryption, Secure Secret Key Sharing, Third Party Auditing.

I. INTRODUCTION

The service over the Internet is provided to end user by CC, which is used to maintain and manage the data is known as Cloud data storage. It helps to back up the data remotely, also the users became available through internet [1]. By using this cloud data storage service, the users can move the data easily without facing any difficulties in direct hardware management since it is user friendly. Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [2] are the best tools to develop the CC vendors, because they provide a vast amount of storage space. The user will get free from the problems which is raised in local data storage and maintenance [3]. Hence, the cloud data storage service neglects the local machine's requirements. While hosting the cloud data, security issues may arise because the data can be accessed or misused by unauthorized which leads to disclose the sensitive information of end user.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Dasari Venkata Ramesh*, Department of Information Technology, Prakasam Engineering College, Kandukur, India.

The cloud data gets discarded or not able to be accessed or rarely accessed by the CSP to save the storage space. The CSP may be honest but it curious sometime because they hide the information about data loss to the end user [4]. Moreover, some security mechanisms have been provided by the data storage services to protect the sensitive and confidential data. Cryptography and Audit Service has been introduced to tighten the security by providing integrity and confidentiality of user's data. The user's data can be verified and ensure the security of data is known Data Auditing process which consists of two process, i.e. private and public auditing. The auditing process can be carried out by either person or organization known as Third Party Auditor (TPA) which also manages the integrity of cloud data. The data can be verified by Data Owner (DO) itself and stored in cloud is known private auditing, which increases the overhead of verification to the client [5]. The CSP assigned the TPA [6] to audit the stored cloud data. This performance of verifying data using TPA [7] is named as Public Auditing. Due to insecure actions happened in auditing the cloud data, the end user come to the conclusion that TPA having excessive skills in auditing process [8]. The log files of data consist of file name, date, time and mode can be maintained and given to the user by TPA. While auditing, TPA may turned by the malicious users to hack the cloud data or complex applications which has been stored in the cloud. To protect the user's cloud data and to mention the correct stage of the file, some levels of auditing has been applied by TPA. The cloud data not only affected by the malicious user or any other adversary, some of the TPA also involved in malicious activity who tied with the CSP [9] which forces the TPA to do unnecessary auditing activity in order to provides enhanced results. The unnecessary auditing had done by the malicious users and also the TPA. To avoid the above mentioned issues, TPA send a notification about the auditing process to client regarding the information of file access and correctness of auditing log [10].

II. LITERATURE REVIEW

Swithin, P. Fiona et al. [11] presented encrypted tags based secure third party auditing scheme with for semantic environment. The proposed methodology consists of four entities such as DOs, data users, TPA and the cloud server, where the DOs upload the private data in the form of encrypted data to ensure the security. The authentication of both DO and data user has been verified by TPA. TPA permits the CSP to produce huge amount of keys by verifying the details of the data user.

But the limitation of the method is that the keys can be produced according to the attributes of each and every end user. El Ghoubach et al [12] shared the delegation key to TPA for auditing process which was assigned this methodology. These keys are used to generate the identities for the data blocks. To get better capability of the auditing mechanism, this method focused on both user and TPA. TPA handles the auditing process in terms of lowest computational and communication cost for multiple users consecutively. Auditing protocol has been used to perform this mechanism in the absence of CSP. Suppose the system failure was happened, TPA were unable to recover the data blocks while auditing. Huiying Hou, Jia Yu, and Rong Hao [13] satisfied the properties of auditing process which was suitable for different security levels with deduplication. Even though, these populated data of cipher text deduplication and unpopulated data of semantic security can be achieved by the proposed scheme. Audit has been done by TPA even if popularity of the data has been changed. The goal of the method was achieved by search the numerical relationship between new and old authenticators. Those new authenticators can be produced by the cloud which depends on the DOs under some constrains of without knowing the private information where, no need of producing new authenticators by the DOs. Yang, Kan, and Xiaohua Jia [14] presented system model of auditing the user data by server and TPA. The metadata was calculated by DOs and also negotiate the keys of TPA and server for cryptography. The DOs chosen to be offline and will not get commit to any auditing queries. The Challenge-response auditing protocol conduct these queries in three phases includes challenge, proof and verification. The correctness of DOs have be checked by TPA and sent it to server. The server need to send a proof of data storage to the client, but it is a time consuming process. Loheswaran, K., and J. Premalatha [15] secured the data in cloud by implementing a renaissance system model. The new model of secured cloud data storage has been proposed which contains four entities such as DOs, the cloud, CSP and TPA. The DO data was stored in server and it was publically audit by TPA which was stored in a vast amount of cloud storage. Here, TPA was independent for DOs and cloud server which was the advantage of this scheme. While doing repairing procedure, a partially trusted proxy agent utilized instead of DOs to reproduce the data blocks. TPA will not create any harmful things to user data privacy. Due to the vulnerability of the TPA, the user's unable to trust the TPA and the trusting of the presented TPA is not tested against the vulnerability issues.

III. OBJECTIVE OF THE RESEARCH

User need to know that, weather the uploaded data in the cloud corrupted or modified by any other unauthorized way. This can be achieved by the proposed trusted third party auditing. Since the CSP is semi trusted, user's data should not affect due to the malfunctions of the CSP. This can be achieved by the proposed proxy re-encryption methodology.

IV. SYSTEM MODEL FOR AUDITING SERVICE

In this research, TPSAS is presented to make sure the security and data integrity, where all the above listed requirements are satisfied. The ultimate aim of this research is to protect stored data that should not modified other than the authorized users. In this paper, two major problems are considered for attaining the integrity of data in the cloud. The first one is, the unauthorized user try to modify the data, which is solved by the proposed TSAS. The second problem considered in this research is, since CSP is semi trustable it can be malfunctioned at any time which can be solved based on the secure secret key sharing algorithm and proxy re-encryption methodology. The secure secret key sharing is implemented based on the Shamir key sharing algorithm and the proxy re-encryption process is implemented based on the bear and lion proxy re-encryption methodology. While auditing, the integrity of remove data is checked by DOs without the knowledge of whole data in most cases. Depends on online and distributed storage systems, the problem of auditing is more signified nowadays. During this time, many protocols has been produced. In many existing protocols, the integrity of remote data can be checked by DOs is known as DO Auditing. TPA provides to prefer the data storage auditing service, named as Third Party Auditing, rather than by DOs. In this type of auditing, the system models have been classified into three entities namely server, DOs and TPA which is shown in Figure 1.

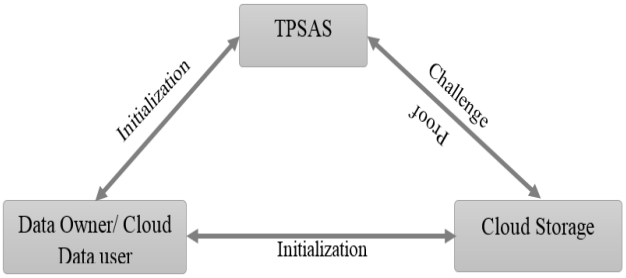

Fig. 1. The overall block diagram of third party storage auditing system.

Figure 1 represents the overall block diagram third party storage auditing system. The overall system has three entities the first one is DO and cloud data users who has accessing of cloud data of DO. The second one is TPA where it records the log reports whomever accessing the file. The third one is CSP where the DO stores the files and the data can be accessed by cloud users. At first, DO begins with the initialization process where, the DO register with the TPA along with the file accessing policy and list of user who has eligible to access the cloud data uploaded by the DO. To store the cloud data in the form of blocks of cipher texts, the DO need to register with CSP. Also, CSP receives a challenge from the TPA for protecting the data security and integrity. Therefore, correctness of proof was checked by using verification process of TPA.

A. Third party data auditing

Challenge-response Auditing Protocol is used to audit the queries by server and TPA, which contains three phases namely challenge, proof and verification of DOs data.

The server uses some set of blocks to store the owner's data in the cloud server. The status of the blocks are stored as log file with the user's identity with time stamp. If the blocks are modified at any time, the status of the blocks are changed in the log file in the proposed Third Party Storage Auditing Service. The proposed TPSAS continuously verifies the status of the data blocks. When the blocks are updated by other than authorized members subsequently, the proposed TPSAS intimates the DO to restore the data. TPA send a challenge request to server for verifying the correctness of DOs data which is stored in cloud. When the request received from TPA, the acknowledgement is generated by server which provides a proof of data storage by checking the status of each blocks of the data storage. The proof reports are send to the TPA, which has the knowledge of set of authorized users of the data block. In verification process, the results are extracted by checking the correctness of proof from server which is initiated by TPA. During the verification process, the TPA verifies status of the block and checks weather the data blocks accessed or modified by any unauthorized user or checks weather the data blocks corrupted by CSP or not. If the data corrupted by the unauthorized access, the TPA sends the request to DO to restore the original data at the cloud server.

B. Secure data storage

According to Bear & Lion proxy re-encryption and Shamir secure secret key sharing algorithm, the integrity and security of user data is maintained. Initially, the data is segregated into set of blocks and each blocks are encrypted with the help of Bear key. Once the plain text encrypted, the Bear key is subjected to Shamir secret key sharing process where the entire Bear key breakdown into N number of parts. Since the CSP is semi trustable, it may subject to malfunction activity. In order to provide the solution for this, cipher text and address of the cipher text also need to be encrypted which is considered as proxy re-encryption. Once cipher text and the location of the cipher text, the encrypted data is stored in the form of re-encrypted at the cloud server and the Lion key also subjected to Shamir secret key sharing process. The detailed description of the Bear and Lion encryption methodology and Shamir secret key sharing algorithm is described in the following sections.

a. Bear and Lion

When combined with cryptographic hash function with stream cipher, the block ciphers of BEAR and LION algorithm was discovered by Ross Anderson and Eli Biham [16] in 1996. Huge various block sizes in the order of 213 to 223 bits were utilized. Independent keys were used twice in hash function and once in stream cipher by LION (inversely) and BEAR. The key may break hash function and stream cipher, when there is an attack happened in any algorithm (i.e. LION/BEAR). Also, this can be proved by the inventors.

The size of block is represented as s and hash function block size is represented as h. The blocks can be divided into A as $A=[x,y]$ with $|x|$ and $|y|=s-h.$

b. BEAR

The two applications such as stream cipher and keyed hash function is used to perform encryption and decryption of BEAR. There are pair of sub keys are available in BEAR algorithms as $B=(B_1,B_2)$ such as $|B_1|>b$ and $|B_2|>b$. Then encryption and decryption are discussed as:

Encryption:

$$x=x\oplus C_{B_1}(y)$$
$$y=y\oplus SC(x)$$
$$x=x\oplus C_{B2}(y)$$

Decryption:

$$x=x\oplus C_{B_2}(y)$$
$$y=x\oplus SC(x)$$
$$x=x\oplus C_{B_2}(y)$$

According to unkeyed hash function C, the keyed hash function C_B satisfies, where the key is append or prepend to message. It is a collision free, one-way and pseudo-random, i.e. it is hard to predict any new input. Also, the stream cipher (SC) is discussed as:

- It can be able to withstand the expansion and key recovery attacks
- It is a pseudo-random.

c. LION

Like BEAR algorithm, the construction of LION is also similar but it uses two applications of stream cipher and one application of hash function. There are pair of sub keys are available as $B=(B_1,B_2)$ such as $|B_1|>b$ and $|b_2|>b$. Then encryption and decryption are discussed as:

Encryption:

$$y=y\oplus SC(x+B_1)$$
$$x=x\oplus C(y)$$
$$y=y\oplus SC(x+B_2)$$

Decryption:

$$y=y\oplus SC(x+B_2)$$
$$x=x\oplus C(y)$$
$$y=y\oplus SC(x+B_2)$$

Again, the hash function (C) is pseudo-random, one-way, collision free and can able to withstand against key recovery attacks and expansion attacks. To ensure the integrity of data, the BEAR and LION algorithm is subjected to Shamir's secret key sharing algorithm. In the following section, the detail description of this algorithm is given.

d. Shamir's Secret Sharing

The secrets are preserved by introducing this method [17], where the secrets are divided into various portions and given to participants. Each user has its own unique part or some parts or all of them requires to rebuild the secret, if needed. The formal descriptions are described as follows [14]:

The data can be divided into various parts such as $d_1, d_2, d_3, .., d_{n-1}, d_n$ the data d can be easily computable by using knowledge of any h or more d_i, otherwise data d will completely leave, i.e. all possible values are equally distributed. This is known as threshold scheme as (h, n). The data d_i can be divided by select a random degree polynomial $q(z) = a_0 + a_1 z + ... + a_{k-1} z^{k-1}$ in which $a_o = d$ and evaluate as

$$d_1 = q(1) ... d_i = q(i) ... d_n = q(n)$$

The coefficients of $q(x)$ can be identified by any subset of key and interpolation, then evaluate $d = q(0)$. To calculate d, knowledge of just $k-1$ of these values are used, which does not suffice. In this approach, threshold scheme are used as (n, n), where each party required to participate in protocol. It is not possible to recover the secret without the co-operation of all parties.

V. EXPERIMENTAL RESULTS

When compared with existing Third Party Medium (TPM) scheme [18], the performance of proposed TPA scheme is evaluated in terms of computation complexity, which is demonstrated in this section. The computation complexity during the authentication generation and challenge generation of proposed TPSAS and existing TPM is computed using $O(n)$, and $O(c)$ respectively. The computation complexity during the proof generation of CSP and proof verification of proposed TPSAS and existing TPM is computed using $O(c)$ where the number of data blocks and challenged blocks are represented as n and c. The performance of the proposed TPSAS algorithm evaluated depends on the authentication cost, proof cost, verification cost. The proof generation cost is computed at the CSP. The verification cost is derived from the proposed TPSAS. The authentication cost represents the required time for encryption process of the BEAR and LION algorithm and Shamir secret sharing algorithm. The comparison of authentication cost of proposed TPSAS algorithm and existing TPM algorithm presented in the following figure 2. By analyzing the figure 2, it is concluded that the proposed TPSAS algorithm performed better than the existing TPM scheme. The authentication cost of the proposed methodology is comparatively lesser than the existing TPM scheme. However, the proposed TPSAS algorithm consists of proxy re-encryption and secret key sharing algorithm, the proposed algorithm requires less authentication cost due to the simple and robust characteristics of the BEAR and LION proxy re-encryption algorithm and Shamir secret key sharing algorithm.

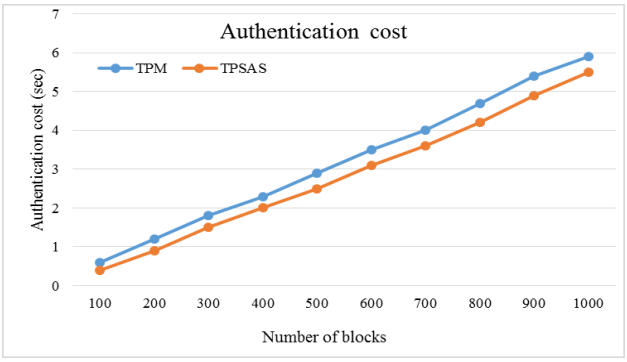

Fig. 2. Comparative analysis of the authentication cost

Figure 3 represents the comparative analysis of proof generation cost proposed TPSAS algorithm and existing TPM algorithm. By analyzing the figure 3, proof generation cost of the proposed TPSAS algorithm is combatively lesser than the existing TPM algorithm. The proposed TPSAS algorithm generates the challenge request to CSP to initiate the process for generating the proof. The CSP generate the proof for every block of data and send the proof generation reports to the TPSAS. Even though, the CSP scans every files and generating proof reports not affecting the computation cost rather than the proposed algorithm minimize the proof generation computation cost which is clearly represented in the figure 3. The comparison of verification cost of proposed TPSAS algorithm and existing TPM algorithm presented in the following figure 4. By analyzing the figure 4, it clearly depicts that the verification cost of the proposed TPSAS algorithm is lesser than the existing TPM algorithm. Hence, the proposed TPSAS algorithm aware of list of authenticated users, and the set initial log reports of each authenticated user, it is very easy to compute the verification process. Hence, the proposed TPSAS methodology maintains the data integrity and performed well in terms of all kinds of cost evaluation.

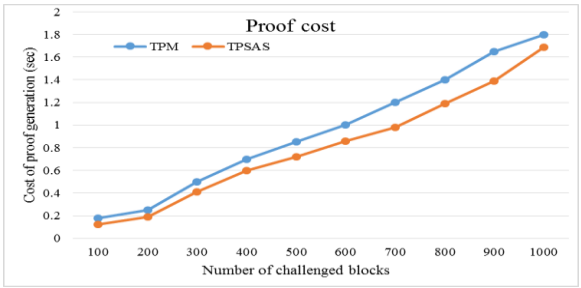

Fig. 3. Comparative analysis of the proof generation cost

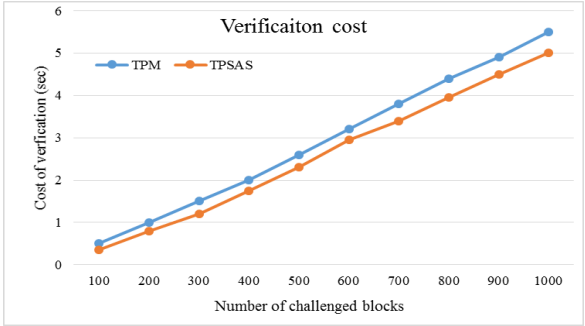

Fig. 4. Comparative analysis of the verification cost

VI. CONCLUSION

The integrity of user's data is ensured by implementing the TPSAS in this research work. Since CSP is semi trustable it can be malfunctioned at any time which affects the integrity of data and this issue is avoided by using the Shamir secure secret key sharing algorithm and Bear & Lion proxy re-encryption methodology. The user data is encrypted based on the Bear & Lion proxy re-encryption algorithm before storing into the cloud which helps to maintain the data security and data integrity. The encryption key is securely shared with the help of Shamir secret key methodology which helps to avoid the unauthenticated access of cloud files. The integrity of data is ensured and proof report on verification process is executed by CSP which is monitored by proposed TPSAS algorithm. When compared with existing TPM scheme, the validation of proposed TPSAS algorithm is calculated and proved that the TPSAS algorithm performed better than the TPM scheme in terms of authentication cost, proof cost and verification cost. For the feature work, rather than continuously auditing the files in the stored environment, it's better to auditing in dynamic which minimize the computation cost.

REFERENCES

1. M. Swapnali, and S. Chaudhari. (2016). Third Party Public Auditing Scheme for Cloud Storage. *International Journal of Procedia Computer Science, 79*, pp. 69-76.
2. Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com, 2008.
3. S. Hiremath, and S. Kunte. (2017). A novel data auditing approach to achieve data privacy and data integrity in cloud computing. 2017 *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT). IEEE*.
4. K. Yang, and X. Jia. (2012). Data storage auditing service in cloud computing: challenges, methods and opportunities. *World Wide Web 15*, pp. 409-428.
5. W. A. Sultan Aldossary. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing. *International Journal of Advanced Computer Science and Applications*, *7*, pp. 485- 498.
6. M. Li, S. Yu, K. Ren, W. Lou. (2010). Securing personal health records in cloud computing: patientcentric and fine-grained data access control in multi-owner settings. *In: Security and Privacy in Communication Networks*, pp. 89–106.
7. L. Li, L. Xu, J. Li, C. Zhang. (2011). Study on the third-party audit in cloud storage service. *In International Conference on Cloud and Service Computing*.
8. C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou. (2013). Privacy-preserving public auditing for secure cloud storage. *IEEE Trans. Comput. 62*, pp. 362–375.
9. S.V. Marshal. (2013). Secure audit service by using TPA for data integrity in cloud system. *Int. J. Innovative Technol. Exploring Eng. (IJITEE), 3.*
10. B. Balusamy, P. Venkatakrishna, A. Vaidhyanathan, M. Ravikumar, N.D. Munisamy. (2015). Enhanced security framework for data integrity using third-party auditing in the cloud system. *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*. Springer, pp. 25-31.
11. P.F. Swithin, M.C. Rathi, S.F. Farveen, and C. Manikandan, (2018). TPA Scheme over Large Scale Cloud System for Achieving Secure and Robust Query Result and Session Verification. *Journal of Network Communications and Emerging Technologies (JNCET), 8*.
12. I. El Ghoubach, R.B. Abbou, and F. Mrabti, (2019). A Secure and Efficient Remote Data Auditing Scheme for Cloud Storage. *Journal of King Saud University-Computer and Information Sciences*.
13. H. Hou, J. Yu, and R. Hao. (2019). Cloud storage auditing with deduplication supporting different security levels according to data popularity. *Journal of Network and Computer Applications, 134*, pp. 26-39.
14. K. Yang, and X. Jia. (2014). TSAS: third-party storage auditing service. In Security for Cloud Storage Systems. Springer.
15. K. Loheswaran, and J. Premalatha. (2016). Renaissance system model improving security and third party auditing in cloud computing. *Wireless Personal Communications, 90*, pp. 1051-1066.
16. R. Anderson, E. Biham. (1996). Two practical and provably secure block ciphers: BEAR and LION. *In: Golmann, D. (ed.), Fast Software Encryption – FSE '96, 1039*, pp. 113–120.
17. A. Shamir. (1979). How to share a secret. *Communications of the ACM 22*, pp. 612–613.
18. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, R. Hao. (2017). Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium. *Journal of Network and Computer Applications 82*, pp. 56-64.