International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Multiple Authority Based Data Fragmentation Technique for Providing Secure Storage in Cloud

Girish Kumar D, Rajashree V Biradar, V C Patil

Abstract: ***The existing works on security storage in cloud computing cause overhead, data correctness issue, key escrow problem, single point of failure and so on. This develops Multiple Authority based Data Fragmentation Technique for providing Secure Storage in Cloud Computing. It aims to avoid the key escrow and single point of failure issues of secure storage. In this technique, the Cloud Service Provider (CSP) provides multiple services for a client, the trusted and verification authorities are responsible for jointly creating the master key and system parameters and the Cloud Data Owner (CDO) encrypts the documents using CP-ABE. In order to provide data recoverability, a file is divided into blocks and sectors. Probabilistic algorithm checks the integrity of fragmented file. By simulating, the proposed technique reduces the overhead and data failures.***

Keywords : Cloud Computing, Storage,Fragmentation

I. INTRODUCTION

Cloud computing(CC) has changed the organizations view on hardware and software. Which offers many facilities such as free services, flexible resources, quick access through the internet and etc. It provides more flexible environment for computation and storage requirements. The aim of CC is to share the resources among the cloud users.

However, data security over the cloud is considered as the main challenge, due to its centralized resources and the different levels of security provided by each cloud provider. Hence it is necessary to provide best potential level of security for users in the cloud [4]. The data which is stored in out sourced servers and may be modified or accessed by un-authorized users, by the CSPs and correctness of data includes verifying integrity of out sourced data which is stored in remote location or server periodically. Some dishonest CSPs may hide the loss of uploaded data from the CDUs, for their own gain. In addition to this, the CSPs may delete some unused data of users to conserve the storage space. Hence the CDOs have to provide assurance to the correctness of the stored data in the servers. [5].

Manuscript published on November 30, 2019.
* Correspondence Author
Mr. Girish Kumar D*, Research Scholar, Department of CSE, BITM, Ballari, Karnataka, India
Dr. Rajashree V Biradar, Professor Department of CSE, BITM, Ballari, Karnataka, India
Dr. V C Patil,[3]Principal, BITM, Ballari, Karnataka, India

The vital challenges of Cloud Storage Security includes: maintaining confidentiality, providing data integrity, data recoverability and vulnerability and avoiding single point of failure. In order to provide integrity, digital signature based schemes are applied. A designated verifier signature is applied in [6] but it uses a session-key for encryption.
A cooperative PDP scheme [11] is presented for verification of data integrity and automatic recovery. But it fails to address the issues of authentication and authorization of shared data.
The private keys of data owners and clients are given by a Trusted Authority (TA)., which leads to a data security risk called as *key-escrow problem.* Most of the researchers used only a single trusted authority for issuing key. Moreover using a single TA will leads to single-point failure and affects performance.

II. RELATED WORK

Sl. No	Authors Name	Title of work	Main contributions	Advantages	Drawbacks
1	Al-Azi et al [5]	New Secure Network CC Storage Architecture	File is encrypted and divided into various sub blocks	Improves reliability, scalability, availability and secured storage	Does not provide integrity verification for the blocks of data
2	Wiei et al [6] [6]	Security and privacy during transmit and at rest	Privacy auditing protocol for cheating discouragement and computation	Provide privacy preservation and integrity	Does not provide confidentiality and access control
3	Chatterje et al [7]	Steganographic Approach using Huffman Coding	New data hiding technique which stores the data into several images	Ensures storage security, provides confidentiality and prevents unauthorized users.	Involves huge storage cost

Sl. No	Authors Name	Title of work	Main contributions	Advantages	Drawbacks
4	Wiang et al [8]	Data Dynamics & Public Auditability for Storage Security	The data integrity of dynamic data is verified	Provides secure storage and integrity	Does not provide privacy preservation, confidentiality and access control
5	Yang et al [9]	Protocol for secure storage & dynamic auditing	Privacy-preserving auditing protocol	Provide privacy preservation and integrity	Does not provide confidentiality and access control
6	Cao et al [10]	Mobile Multi Cloud Data Integrity Verification (MMCDIV)	Applies BLS short signature scheme, Homomorphic verifiable response and constructs Merkle hash tree	Reduces communicati on overhead	Does not provide privacy preservation, confidentiality and access control
7	Zhu et al [11]	Cooperative PDP	Homomorphic encryption for verifying the response and hash index	Provides strong Integrity	Does not provide privacy preservation, confidentiality and access control
8	Luo et al [15]	HMA-ABE	ABE using multi authority, friend discovery schemes	Provides confidentialit y and secure access control	Does not provide privacy preservation and integrity
9	Fen et al [16]	Cloud service selection multi-dimensional trust-aware	Selects the most trustworthy cloud service	Detects misbehaving users and CSPs	Does not provide privacy preservation, confidentiality and integrity

Table 2.1 **presents the related works done along with their contributions, advantages and drawbacks.**

III. RELIABLE & SECURE STORAGE

3.1 Overview

In this paper, we propose a Multiple Authority based Data Fragmentation Technique for providing Secure Storage in Cloud Computing. The technique consists of CSP (Cloud Server Provider), CDO (Cloud Data Owners) , CDU (Cloud Data Users), TA (Trusted Authority) and Verification Authority (VA). CDU downloads the fragmented file from CSP. Both TA & VA jointly creates system parameters and master key. Finally the user will construct the entire secret key.

3.2 System Model

The functionalities of these entities are as follows:

CSP: It acts as the main authority of cloud servers, semi-trusted entity which provides various services to clients.

CDO: It acts as the data owners of the files.

CDU: It accesses the file stored in cloud system and downloads it.

TA & VA: It is a semi-trusted entities.

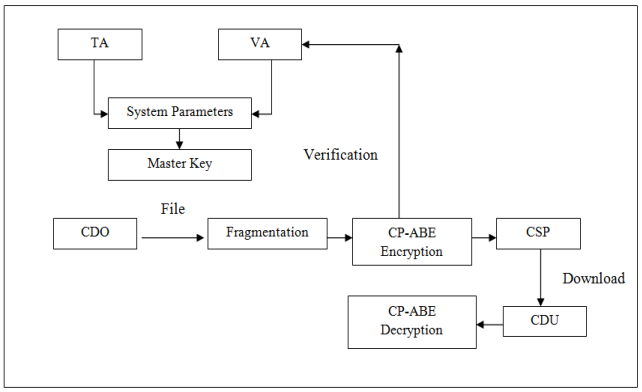

Figure 3.1: System Model

3.3 Collaborative Generation of System Parameter and Master Key

Whenever a client wish to join the cloud, TA will accept user registration which includes name, password, his role (position or designation in case of any organization, subscribed or non-subscribed in case of a service. TA assigns weights for each attributes X to the user based on role. TA and VA co-operate with each other to generate a master key and system parameter to user.

Algorithm-1

1. TA accept k and selects random $\eta_1, \lambda \in Z_p$
2. TA computes $K_{ms1} = \{\eta_1, \lambda\}$
3. TA computes $h = g^{\lambda}$ and $v_1 = e(g,g)^{\eta 1}$
4. TA obtains $SP_1 = \{G_0, g, h, v_1\}$
5. TA transmits K_{ms1} and SP_1 to VA
6. VA accept k and selects random $\eta_2 \in Z_p$
7. VA computes $v_2 = e(g,g)^{\eta 2}$
8. VA obtains $SP_2 = \{v_2\}$
9. VA computes $K_{ms2} = \{\eta_2\}$
10. VA transmits K_{ms2} and SP_2 to TA
11. Then both TA and VA generate CP and K_{ms} as

$$CP = \{G_0, h, (v_1.v_2)\}$$

$$K_{ms} = \{(\eta_1, \lambda), (\eta_2)\},$$

3.4 Creating Fragment Structure for Files

In this scheme, each file is divided into sub groups at each level. Then a fragment structure is created for each file of the group.

Algorithm-2

1. For each $F_i \in W$,
2. CDO selects a specific file F_i to uploading
3. CDO divides the file F_i as $\{B_{i1}, B_{i2}, \ldots\ldots B_{in}\}$
4. Each block B_{ij} is represented as $\{S_{ij}^1, S_{ij}^2, \ldots S_{ij}^k\}$, j=1,2….n
5. Select random secrets $\{T_1, T_2, \ldots T_k\}$ for F_i
6. Create a tag β_{ij} for each B_{ij} as
7. $\xi^{(1)} = H.\sum_{m=1}^{k} T_m(F_i)$
8. $\xi^{(2)} = H_{\xi(1)}(C_g)$
9. $\xi^{(3)} = H_{\xi(2)}(B_{ij})$
10. $u_m = g^{T_m}$, m=1,2,…k
11. $\beta_{ij} = \left(\xi^{(3)}\right)^{\alpha 1}.\left(\prod_{m=1}^{k} u_m^{B_{ij}}\right)^{\alpha 2}$
12. Form the fragment structure as $\{(B_{i1}, \beta_{i1}), (B_{i2}, \beta_{i2}), \ldots (B_{in}, \beta_{in})\}$
13. CDO uploads fragmented F_i into CSPs
14. End For

3.5 Verification of Integrity

The fragment structure then probabilistic verification technique is used to check the intigrity of fragmented file.

Algorithm-3

1. If a F_REQ has been received from the CDU, then
2. CA initiates V_REQ to VA
3. VA computes the challenge
4. IP = { B_{ij} , c_j}
5. VA returns {IP} to CA
6. CA forwards {IP} to each CSP_k
7. Each CSP_k returns R_k to CA
8. If CA receives R_k, then
9. CA aggregates $\{R_k, k=1,2\ldots r\}$ into R using homomorphic property.
10. CA transmits R to VA
11. End if
12. VA checks the response R and checks the integrity of blocks
13. If integrity is failed for any $b_{ij} \in CSP_k$, then
14. That CSP is considered as not trusted
15. End if
16. End if

3.6 CP-ABE based Encryption/Decryption

Algorithm-4

1. For each file F_i
2. CDO encrypts each block b_{ij} as
3. $Enc(b_{ij}) = (K_{pub}, b_{ij}, WA)$
4. CDO transmits $Enc(b_{ij})$ to CSP_k
5. End For
6. CDU generates K_{pr} as
   $K_{pr} = Keygen(K_{pub}, K_{ms}, A_i)$
7. CDU send request for File F_r to CA
8. CA checks matching CSP for F_r
9. If CSP_x found, then
10. CSP_x transmits $Enc(b_{rj})$ of F_r to CDU
11. End if
12. CDU downloads $Enc(b_{rj})$ from CSP_x
13. If K_{pr} satisfies WA, then
14. $Dec(b_{rj}) = Decrypt(K_{pub}, Enc(b_{rj}), K_{pr})$
15. End if

In this algorithm, using the weighed access policy WA and the public key, the CSO encrypts all blocks of a file Fi and transmits the encrypted blocks to CSP. The CDU creates its own secret key by using public key, its attribute A_i. It downloads the encrypted blocks $Encr(b_{rj})$ of the requested file from the corresponding CSP. If secret key matches with the weighted accessing policy WA, CDU will download the file. If there is no matches with any access policy of WA, CDU cannot decrypt the file.

IV. EXPERIMENTAL EVALUATION

To validate the proposed multiple authority based data fragmentation technique for providing secure storage in CC, CP-ABE and JPBC is implemented[14]. To check the results of RSSCTA, we have implemented CP-ABE [13] & HM-ABE [15] techniques. In traditional CP-ABE, only a single authority is used for generation of secret key. Moreover, accessing policies will consume more storage space and hence involve high encrypting and decrypting time. In the other side, the HM-ABE scheme has multiple authorities but it did not possess integrity verification and block recovery mechanism. The proposed RSSCTA provides integrity and block recovery. Moreover, the weighted access policy of RSSCTA consumes considerably less space.
The experiment is conducted on windows system and all the results are obtained from 10 trails.

V. RESULTS

The experimental results are obtained by changing the file size from 1MB to 5MB.
The time involved in encrypting and decrypting process are measured. Figure 3 and 4 decipits the result of encryption and decryption.

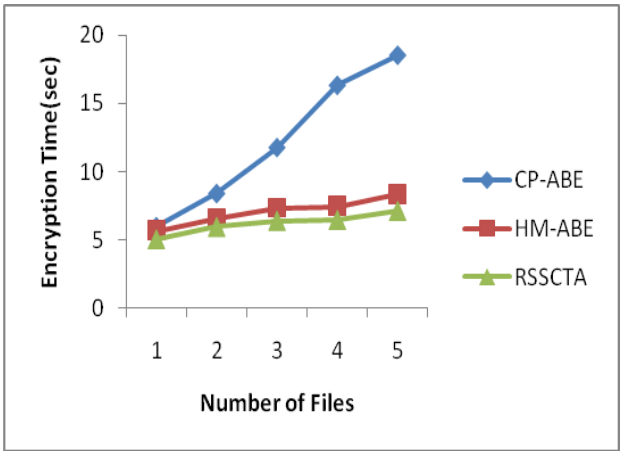

Figure 3 Encryption time

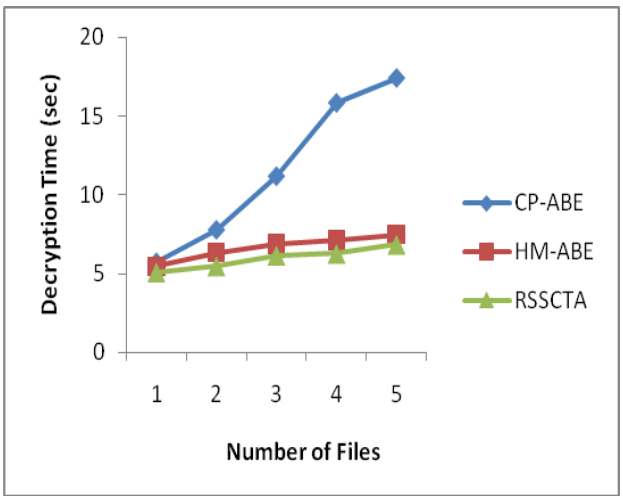

Figure 4 Decryption time

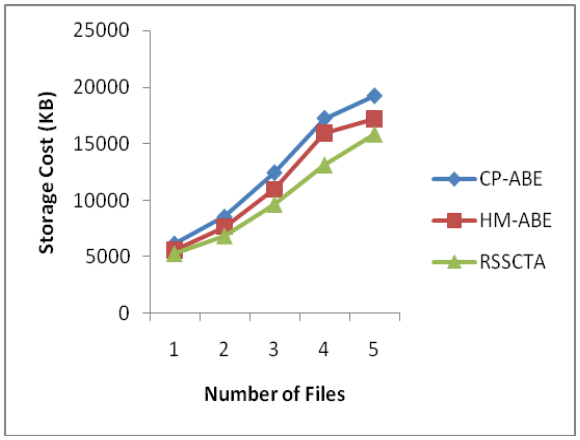

Figure 5 Storage Cost

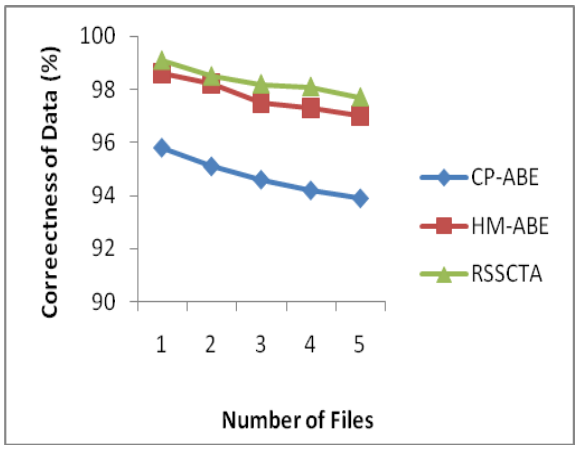

Figure 6 Data Correctness

VI. CONCLUSION

In this paper, a Multiple Authority based Data Fragmentation Technique for providing Secure Storage in CC is proposed, which provides security for the out sourced data in an un trusted cloud storage. The proposed technique guarantees that the data is secure, Since only the authorized data users can download the file with the help of trusted authorities and this technique also supports dynamic operations for the data owners such that he can modify the contents of the file which is stored in remote server.

REFERENCES

1. Naresh vurukonda and B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing", Procedia Computer Science, Elsevier, 92 (2016) 128 – 135.
2. Yunchuan Sun,Junsheng Zhang,Yongping Xiong and Guangyu Zhu, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, Hindawi,Volume 2014, Article ID 190903, 9 pages
3. Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos, "Security in Cloud Computing: Opportunities and Challenges", Information Sciences (2015), Elsevier, doi: http://dx.doi.org/10.1016/j.ins.2015.01.025.
4. Almokhtar Ait El Mrabti, Najim Ammari and Mina De Montfort, "New mechanism for Cloud Computing Storage Security", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 7, 2016.
5. Fawaz S. Al-Anzi, Ayed A. Salman, Noby K. Jacob, "New Proposed Robust, Scalable and Secure Network Cloud Computing Storage Architecture", Journal of Software Engineering and Applications, 2014, 7, 347-353.
6. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing", Information Sciences, Elsevier, 2013.
7. Trijit Chatterjee,Mrinal Kanti Sarkar and Dr. V S Dhaka, "Steganographic Approach to Ensure Data Storage Security in Cloud Computing Using Huffman Coding (SAHC)", International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015.
8. Qian Wang,Cong Wang,Kui Ren,Wenjing Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing",ESORICS'09,2009.
9. Kan Yang and Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing",IEEE,2012,D.O.I:10.1109/TPDS.2012.278.
10. .Laicheng Cao, Wenwen He, Xian Guo, and Tao Feng, "A Scheme for Verification on Data Integrity in Mobile Multicloud Computing Environment", Mathematical Problems in Engineering, Volume 2016, Hindawi, Article ID 9267608, 6 pages.
11. Yan Zhu,Hongxin Hu,Gail-Joon Ahn and Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 12, December 2012.
12. Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, and Weixin Xie," Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 8, August 2016
13. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
14. A. De Caro and V. Iovino, "jPBC: Java pairing based cryptography," in Proc. IEEE Symp. Comput. Commun., Jun./Jul. 2011, pp. 850–855.
15. Entao Luo, Qin Liu and Guojun Wang, "Hierarchical Multi-Authority and Attribute-Based Encryption Friend Discovery Scheme in Mobile Social Networks", IEEE Communications Letters, Vol. 20, No. 9, September 2016.
16. Fan, Wenjuan,Yang, Shanlin, Perros, Harry Pei and Jun, "A Multi-dimensional trust-aware cloud service selection mechanism based on Evidential Reasoning Approach", International Journal of Automation and ComputingApril 2015, Volume 12, Issue 2, pp 208–219
17. Rizwana Shaikha and M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", Procedia Computer Science 45 (2015) 380 – 389.
18. .Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi,Andrea Margheri, and Vladimiro Sassone, "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments", In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), 2017,Venice, Italy.