International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Committed Data Destitution in Cloud Using Cipher Text Encryption Methods

Bikkina Lalitha Bhavani & J.Malathi

[1]Assistant Professor, Department of IT, Sir. C.R.Reddy Engineering College, Eluru AP.

[2] Assistant Professor, Department of IT, Sir. C.R.Reddy Engineering College, Eluru AP.

Email:karuturi.lalithacse@gmail.com[1], malathi.komma@gmail.com[2]

ABSTRACT: *Cloud Computing is latest technologies which is going to play a vital role in the next generation of computer engineering field. The increased security and flexibility provided by the cloud computing has reduced the costs to a greater extent and therefore the technology has gained wide acceptance. Data access control is a successful use to ensure the data security in the cloud. The data access control is demanding and data security has a major method in data storing on cloud for this data access control in cloud storage a Cipher text-Policy Attribute based Encryption (CP-ABE) scheme is take to be the most appropriate technology its access the data owner to have a control on right to use policies. We proposed the security of ID-based ring mark by giving forward top master key of any client has been bargained in addition the method of decrypting and encrypting all the shared data can make certain forward secrecy. This proposal has advantage requisites of functionality and competence and thus is possible for a realistic and producing good result with effective cost benefits this property is particularly imperative to any expansive scale data conveyance framework. Only a constant number of simple operations for PKG and users are left to perform locally. The proposed method is introduced outsourcing computation into IBE destitution method in the security definition of outsourced destitution IBE for the first time to the best of our data and the user-specified end time the data in cloud server will be securely self-destructed.*

Index Terms: - Cloud Computing, Self-Destruction, Identity Based Encryption (IBE), Revocation, Outsourcing, cipher text, security issues.

1. INTRODUCTION

Cloud Computing is one of internet based computing. Most of time data is share using cloud computing. Cloud is big area to take any type of data, and information [1]. We all share the data based on cloud computing. Cloud provides the method for shared computer processing resources. Security is important in today's environment. Provide extra security many data sharing in cloud computing is one of the big challenge. Encryption technique is used for sharing secure data between senders to receive [2]. Cipher text-Policy Attribute based Encryption (CP-ABE) consisting an authority which is responsible for maintaining the attribute management and key distribution .the authority is human resource in the company the data owners will defined their access policies over the attribute and store the data on the cloud in an encrypted format and each user secret key reflecting its attributes so the user can decrypt the data only if its satisfied the access policies [3]. There are two types of CPABE systems: single-authority CP-ABE where all attributes are managed by a single authority and multi-authority CPABE where attributes are from different domains and managed by different authorities [4]. Also to improve the cloud storage space a secure data self-destructing system in cloud computing is proposed. In this system is private key is connected with a time instant every cipher text is labeled with a time interval [5]. If the time instant is in the access time interval and the identities associated with the cipher text satisfy the key access structure then the cipher text is decrypted. In general the owner has the right to specify that certain sensitive information is only valid for a limited period of time [6].

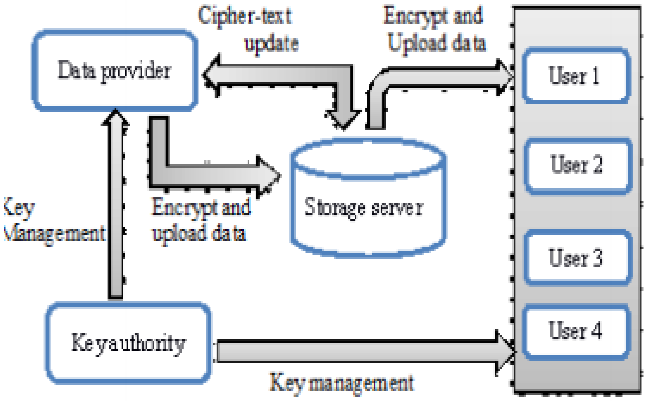


Figure-1: Cipher Text Model

2. RELATED WORK

Public key and private key are used to encryption and decryption respectively in this paper AES algorithm as well as KUNode algorithm is used secrecy or backward secrecy provided for security [7]. Forward secrecy is used for advanced security the previous and subsequent data so that revocable identity based encryption methods is used. Data providers upload the files into storage server using the encryption methods. For the encryption key is used and this key provide by the key authority. Storage server stores the files is uploaded by data provider [8]. And users download the file as per their need. We resolve this challenging method by considering more practical scenarios in which semi trustable on-line proxy servers are available. We achieve this by uniquely integrating the method of proxy re-encryption with CP-ABE and enable the authority to delegate most of laborious tasks to proxy servers [9]. Formal analysis our proposed scheme is provably secure is chosen cipher text attacks. In addition we show that our methods is applicable to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart. We propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming a variant of the computational Diffie-Hellman problem [10]. Our system is based on bilinear maps between groups. We give precise definitions for secure identity based encryption schemes and give several applications for such systems.

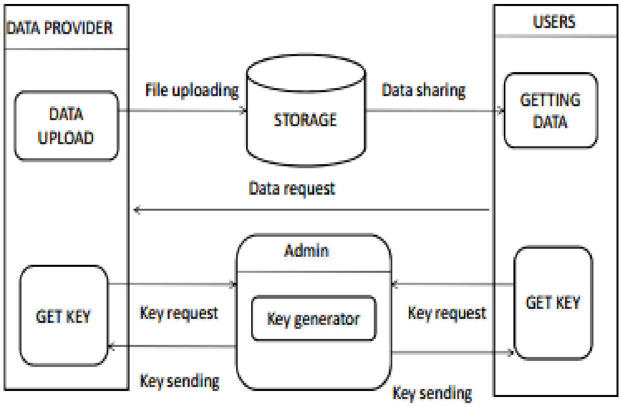
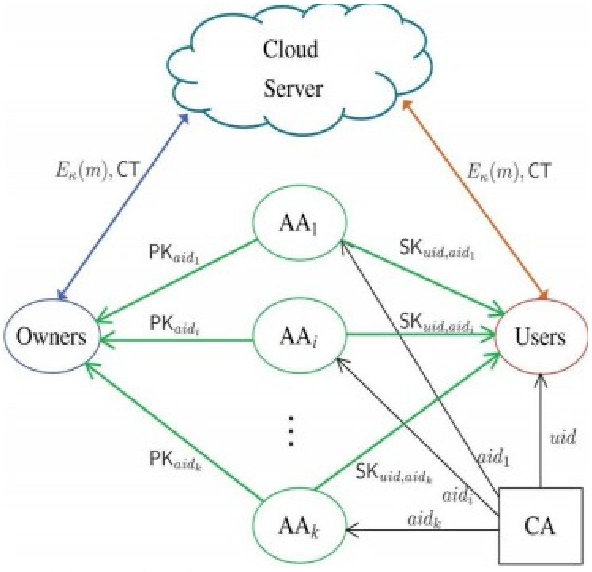


Fig No 2. User Getting Key

3. SYSTEM ARCHITECTURE

This system architecture consisting of five entities such as, 1.certificate authority (CA), 2.cloud owner, 3.attribute authority 4.cloud user 5.cloud server. The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users [11]. The CA is any attribute management and the creation of secret keys that are associated with attributes. In previous work the system stores the data at cloud server and the user itself has delete the data stored in cloud if he no longer needed the data, it increases overhead of user and also uses more space at cloud server to overcome the drawback of previous system the system proposes data self distractive scheme in this user upload the data in cloud server for specific time duration at cloud server data is valid for only one year from start date to end date specified by user after completion of time period data is self-destructed from the cloud and it frees the space at cloud server [12].



4. PROPOSED SYSTEM

The user registers to server and then login with valid username and password in to system. After login user request for keys to KU-CSP [13]. The user encrypts the files using the keys and uploaded these files in cloud server for specific time interval and become free from the burden. It is treated as a public cloud is run another party to provide the capability of computing to PKG for regulating the network by using the services. The KU-CSP is given away from the users the PKG this PKG helps to reduce the storage cost and find the users only by giving the flexibility and also the temporary extension to the user infrastructure [14]. At cloud server if the specified time for the file is end then the file is destructed from the server and it is no longer available for users. To ensure that the newly joined user is sufficient attributes is decrypt the previous data which is published before it joined the system all the cipher texts associated with the revoked attribute is required to be updated to the latest version [15].Further it consists of three requirements for such model the requirements are as follows:

1. Any one of the KU-CSP must be honest

2. There might be the computational complexities to obtain the effect to the revocation a true KU-CSP is needed.

3. The PKG run time might be much smaller the needed to directly act or carry out revocation process.

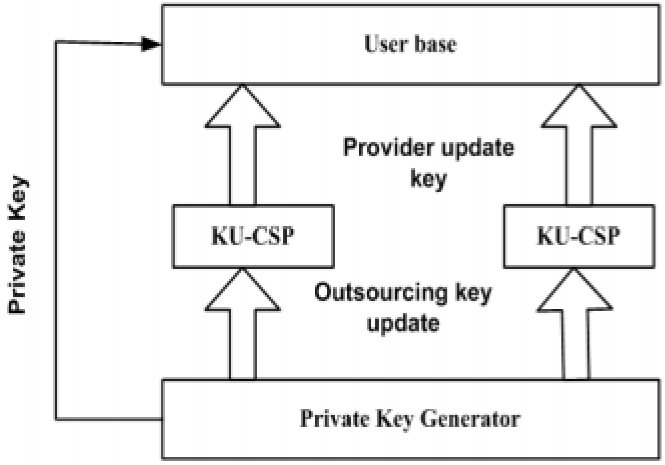


Fig 3: Proposed System

5. ALGORITHMS

In which every user key is associated with an access tree and each leaf node is associated with a time instant the data owner encrypts his data to share with users in the system. As the logical expression of the access tree is signify any desired data set with any time interval it is attain fine-grained access control. The cipher text is decrypted this cipher text will be self-destructed and no one can decrypt it because of the expiration of the secure key.

A. Mathematical Model:

System S is represented as S= {U, CS, KU-CSP}

1) **User US** = {R, L, Q, E, V} Where, R= Registration Process L= Login Process Q= Key Request Process E= File Encryption Process V= Revocation Process

2) **KU-CSP**={PK,SK} Key Generation PK={pk1, pk2, pk3 ...pkn} Where PK is the set of generate public keys. SK= {sk1, sk2, sk3 ...skn} Where SK is the set of generate private keys related to public key.

3) **Cloud Server** CS ={U, D} Where, U = Upload file D= {T, F} Where, D = Self-Destructive Process T=Time Interval F=Number of files

B. Algorithm

1) **Setup ( ):** PKG run the setup algorithm. It chooses a random generator g 2R G as well as a random integer x 2R Zq and sets g1 = gx. Then finally output the public key PK= (g; g1; g2; H1; H2) and the master key MK = x.

2) **Key Gen (MK, ID, RL, TL, and PK):** PKG firstly checks whether their quest identity ID exists in RL, for each user private key request on identity ID, PKG reads the current time period Ti from TL. Accordingly, it randomly selects Ti 2R Zq and computes, where and finally, output SKID = (IK [ID]; TK [ID] Ti) and OKId = x2. [16].

3) **Encrypt (M, ID, Ti+, and PK):** Assume a user needs to encrypt message M under identity ID and time Ti period. He chooses a random value s 2R Zq and computes, C0 = Me (g1; g2) s; C1 = gs; EID = (H1 (ID)) s and Finally, publish the cipher text as CT = (C0; C1; EID; ETi).

4) **Decrypt (CT; SKID; PK):** Assume that the cipher text CT is encrypted under ID and Ti, and the user private key SKID = (IK[ID];

TK[ID]Ti), where IK[ID] = (d0; d1) and TK[ID]Ti = (dTi0; dTi1).

5) **Revoke (RL; TL; {IDi1; Idi2; dik}):** If users with identities in the set {IDi1; Idi2; ::::Idik} are to be revoked at time period Ti, PKG updates the revocation list as RL0 = RL{IDi1; Idi2; ::::Idik} as well as the time list.

6) Key Update (RL; ID; Ti+1; OKID): Upon receiving a key update request on ID , KU-CSP firstly checks whether ID exists in the revocation list RL , if so KU-CSP returns and key-update is terminated. It randomly selects Ti+1 2R Zq.

7) Data self-destruction after end: Previously the current time instant tx lags behind after the threshold value (expiration time) of the valid time interval tx, the user cannot obtain the true private key SK. Therefore, the cipher text CT is not capable to be decrypted in polynomial time, ease the self destruction of the shared data after end [17].

6. EXPECTED RESULT

The system used Net beans (version 8.0) tool for development and Java framework on Windows platform as a front end. Any standard machine is capable of running the application. The system doesn't need any specific hardware to run.

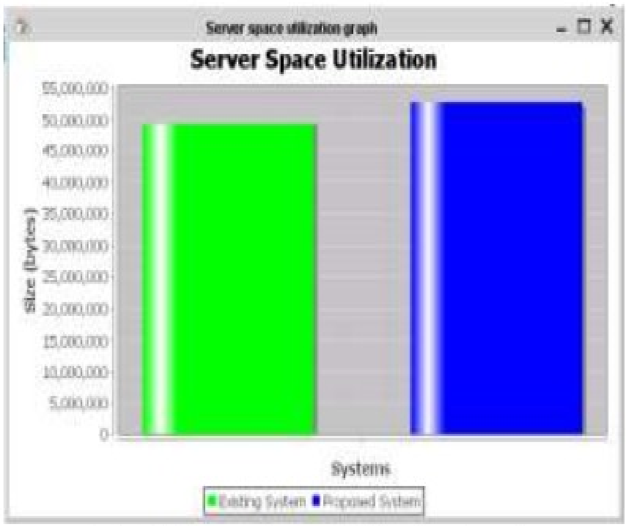


Fig 4. Server Space Utilization Graph

The server space utilization graph comparing the existing system and proposed system in which we can see that the proposed system use server space more efficiently.

7. CONCLUSION

Many recent challenges have appeared with the fast growth of adaptable cloud services. One of the most significant problems is how to securely delete the outsourced data stored in the cloud severs. It provides constant efficiency to compute the PKG and size of private key at the user. 2. It offers convenience since the user may not contact the PKG at the time of key updating and there is no need of user authentication between the user and the CSP. CPABE is an efficient technique, which can be applied in any remote storage systems and online social networks. There is No secure channel or user authentication is required during key-update between user and KU-CSP, also with the help of KU-CSP, the system has features such as; steady effectiveness for both computations at PKG and private key size at user.

8. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[3] J. Bettencourt, A. Sahai, and B. Waters,„„CiphertextPolicy Attribute-Based Encryption,‟‟in Proc. IEEE Symp. Security and privacy (S&P‟07),2007, pp. 321-334.

[4]B. Waters, „„Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,‟‟ in Proc. 4th Int‟l Conf. Practice and Theory in Public Key Cryptography (PKC‟11), 2011, pp. 53-70.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption,"in Advances in Cryptology (EUROCRYPT‟05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557-557.

[6] J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryp-tion of attribute based encryption with mapreduce," in Information and Communications Security. Berlin, Heidel-berg:Springer, 2012, vol. 7618, pp. 191-201.

[7] A preliminary version of this paper appears in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008. This is the full version.

[8] A preliminary version of this paper appears in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008. This is the full version

[9] A.B. Lewko and B. Waters, „„Decentralizing AttributeBased Encryption,‟‟ in Proc. Advances in CryptologyEUROCRYPT‟11, 2011, pp. 568-588.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, ,,,,Attribute Based Data Sharing with Attribute Revocation,‘‘‘‘ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS‘‘10), 2010, pp. 261-270

[11] C. Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2011, pp. 820–828.

[12] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” in Proc. 20th USENIX Conf. Security (SEC‘‘11), 2011, pp. 34–34.

[13] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, “Identity-Based Encryption with Outsourced Revocation in Cloud Computing”, in IEEE transactions on computers, vol. 64, no. 2, february 2015.

[14] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,” In Advances in Cryptology (CRYPTO98). New York, NY, USA:Springer, 1998, pp. 137-152.

[15] J. Bethencourt, A. Sahai, and B. Waters,,,,,,CiphertextPolicy Attribute-Based Encryption,‘‘‘‘in Proc. IEEE Symp. Security and privacy (S&P‘‘07),2007, pp. 321-334

[16] A. Sahai and B. Waters, “Fuzzy identity-based encryption,”in Advances in Cryptology (EUROCRYPT‘‘05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557-557.

[17] J. Li, C. Jia, J. Li, and X. Chen, “Outsourcing encryp-tion of attribute based encryption with mapreduce,” in Information and Communications Security. Berlin, Heidel-berg:Springer, 2012, vol. 7618, pp. 191-201.