Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

An Efficient Lightweight Secure Data Sharing Scheme for Mobile Cloud Environment

T. Neha Singh[1], K. Mamatha[2]

[1, 2] Asst. Prof, Dept. of CSE, Malla Reddy Institute of Technology & Science, Secunderabad.

Abstract: *We propose a lightweight data sharing scheme (LDSS) for versatile distributed computing. It receives CPABE, an entrance control advancement used as a piece of normal cloud condition, yet changes the structure of access control tree to influence it to suitable for versatile cloud circumstances. LDSS moves a gigantic piece of the computational genuine access control tree change in CP-ABE from PDAs to external go-between servers. Besides, to diminish the customer revocation cost, it familiarizes quality depiction fields with complete sluggish disavowal, which is a thorny issue in program based CP-ABE structures.*

Keywords: *Data encryption, access control,user revocation*

1. Introduction

The best in class advantage organization/get the chance to control frameworks gave by the CSP are either not satisfactory or not especially favorable. They can't meet each one of the necessities of data proprietors. To begin with, when people exchange their data archives onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may watch out for customer data for its business favorable circumstances and in addition diverse reasons. Second, people need to send watchword to each datum customer if they simply need to share the encoded data with particular customers, which is to a great degree clumsy. To enhance the advantage organization, the data proprietor can confine data customers into different social events and send mystery key to the get-togethers which they have to share the data. Regardless, this approach requires fine-grained get the opportunity to control. In the two cases, mystery word organization is a noteworthy issue.

2. Literature Survey

The author, Jia W, Zhu H (ET .AL), AIM we anticipate a safe portable client based information benefit system (SDSM) to give mystery and fine-grained get the chance to control for data set away in the cloud. This framework enables the adaptable customers to welcome safe outsourced data organizations at a constrained security organization overhead. The centre idea of SDSM is that SDSM outsources the data and also the security organization to the versatile cloud in a confide in way. Our examination shows that the proposed instrument has numerous central focuses over the current regular systems, for instance, cut down overhead and favorable revive, which could better cook the necessities in adaptable disseminated registering circumstances.

The author, zhou z, (ET .AL), AIM we demonstrate an extensive security data request for framework for versatile appropriated processing. Our answer focuses on the going with two research headings: First, we exhibit a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to ensure detecting information. Utilizing PP-CP-ABE, light-weight gadgets can safely outsource overwhelming encryption and decoding operations to cloud specialist organizations, without uncovering the information content. Second, we propose an Attribute Based Data Storage (ABDS) framework as a cryptographic gathering based access control component.

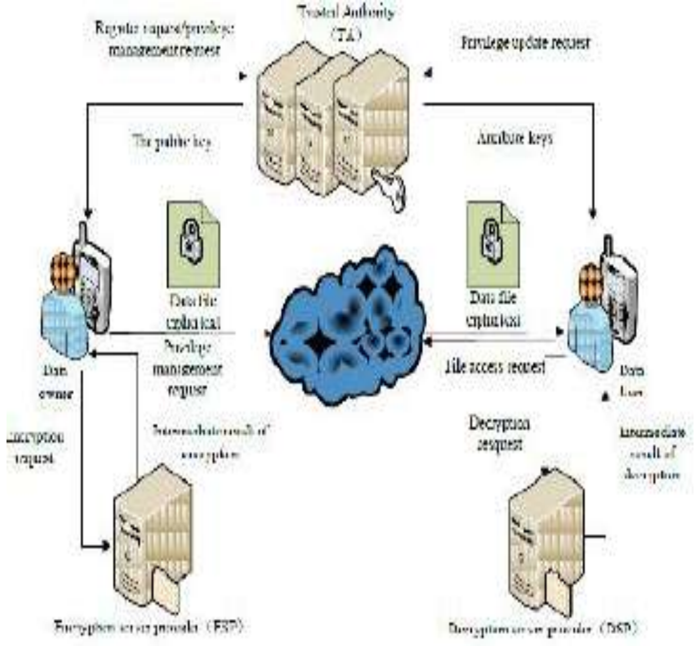
3. Problem Definition

With the advancement of distributed processing and the predominance of splendid PDAs, people are consistently getting adjusted to some other time of data sharing model in which the data is secured on the cloud and the phones are used to store/recuperate the data from the cloud. Ordinarily, PDAs simply have confined storage space and figuring power. Suddenly, the cloud has tremendous measure of advantages. In such a circumstance, to finish the worthy execution, it is fundamental to use the benefits gave by the cloud pro association to store and offer the data.

4. Proposed Approach

Clearly, to deal with the above issues, individual delicate data should be mixed before exchanged onto the cloud with the objective that the data is secure against the CSP. In any case, the data encryption brings new issues. Well-ordered guidelines to give capable access control framework on figure content unscrambling with the objective that select the affirmed customers can get to the plaintext data is trying. Moreover, system must offer data proprietor’s fruitful customer advantage organization capacity, so they can permit/deny data get to benefits easily on the data customers. There have been significant analyses on the issue of data get the opportunity to control over figure content.

System Architecture


Trusted Authority
(TA)
Regular request/privilege management request
Privilege update request
The public key
Attribute keys
Data file ciphertext
Privilege management request
Data owner
Data file ciphertext
File access request
Data user
Encryption request
Intermediate result of encryption
Decryption request
Intermediate result of decryption
Encryption service provider (ESP)
Decryption service provider (DSP)

5. Proposed Methodology

1. Content Encryption and Decryption User encoded the plain content to scrambled arrangement and transferred to the cloud. The encryption is finished by utilizing a secret word. Just utilizing this watchword no one but anybody can decode the content. The client transfer the secret word additionally incorporates with scrambled information. The trusted specialist id in charge of passing the secret key to the requested for client

2. Image Encryption and decoding Like the same as the picture encryption is additionally done. Furthermore, the scrambled pictures and secret key will likewise be transferred to the cloud. The trusted expert id in charge of passing the secret word to the requested for client

3. Text Request Any client can see the document transferred in the server. Every one of the documents are in encoded organize. Client cannot see the documents without know the secret key. For see the document first client need to request for the password to Trusted Authority. TheAuthority checks the client and gives the watchword to legitimate client.

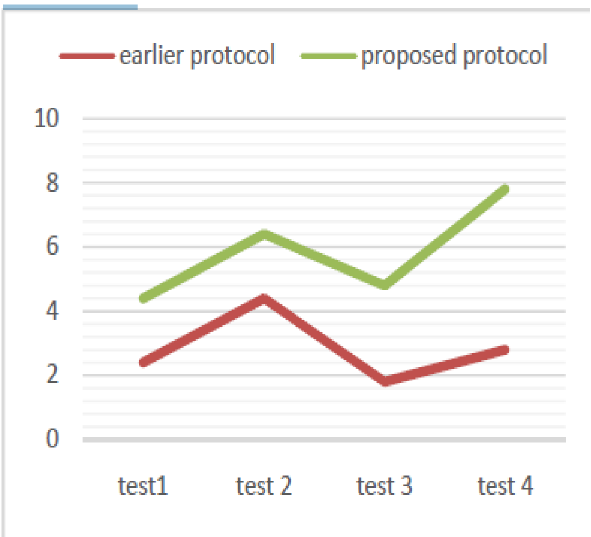
4. Image request Image request for is likewise same as the Text Request. The rundown of pictures can see in the application. Be that as it may, client can just view the pictures in the wake of getting the secret key from put stock in specialist

5. View Encrypted Data The client transferred scrambled information can be seen in the server side. The trusted specialist go about as server they have the duty to give secret word to the requested for client.

6. View user request After client see the encoded information they can request for the secret word for scrambled information. This client demand can be see in the trusted specialist

7. Provide password After view the demand Trusted expert approving the client and if the client is substantial the Trusted specialist give password to the requested for document by means of email. Utilizing this secret word client can unscramble the document.

Results



The result is passed on in java. At long last the proposed thinking displays skilled execution to the degree security and correspondence and furthermore include overhead showed up diversely connection to before system.

6. Conclusion

We propose LDSS to address this issue. It shows a novel LDSS-CP-ABE calculation to move noteworthy estimation overhead from phones onto go-between servers, thus it can deal with the secured data sharing issue in flexible cloud. The exploratory results show that LDSS can ensure data security in convenient cloud and lessening the overhead on customers' side in flexible cloud. Later on work, we will design better approaches to manage ensure data uprightness.

References

[1] Stehlé D, Steinfeld R. Faster fullyhomomorphic encryption. in: Proceedings of 16thInternational Conference on the Theory andApplication of Cryptology and InformationSecurity. Singapore: Springer press, pp.377-394,2010.

[2] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al.Fully secure key- policy attribute-based encryptionwith constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium onInformation, Computer and CommunicationsSecurity (ASIACCS), pp. 239-248, Jun. 2014.

[3] Bethencourt J, Sahai A, Waters B. Ciphertextpolicyattribute- based encryption. in: Proceedingsof the 2007 IEEE Symposium on Security andPrivacy (SP). Washington, USA: IEEE ComputerSociety, pp. 321-334, 2007.

[4] Shi E, Bethencourt J, Chan T H H, et al. Multidimensionalrange query over encrypted data. in:Proceedings of Symposium on Security andPrivacy (SP), IEEE press, 2007. 350- 364

[5] Cong Wang, KuiRen, Shucheng Yu, andKarthikMahendraRajeUrs. Achieving Usable andPrivacy-assured Similarity Search over OutsourcedCloud Data. IEEE INFOCOM 2012, Orlando,Florida, March 25-30, 2012

[6] Yu S., Wang C., Ren K., Lou W. AchievingSecure, Scalable, and Fine-grained Data AccessControl in Cloud Computing. INFOCOM 2010, pp.534-542, 2010

[7] Kan Yang, XiaohuaJia, KuiRen, Bo Zhang,RuitaoXie: DAC- MACS: Effective Data AccessControl for Multiauthority Cloud Storage Systems.IEEE Transactions on Information Forensics andSecurity, Vol. 8, No. 11, pp.1790-1801, 2013.

[8] Gentry C, Halevi S. Implementing gentry'sfully-homomorphic encryption scheme. in:Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148,2011.

[9] Brakerski Z, Vaikuntanathan V. Efficient fullyhomomorphic encryption from (standard) LWE. in:Proceeding of IEEE Symposium on Foundations ofComputer Science. California, USA: IEEE press,pp. 97-106, Oct. 2011.

[10] Qihua Wang, Hongxia Jin. "Data leakagemitigation for discertionary access control incollaboration clouds". the 16th ACM Symposiumon Access Control Models and Technologies(SACMAT), pp.103-122, Jun. 2011.

[11] Adam Skillen and Mohammad Mannan. OnImplementing Deniable Storage Encryption forMobile Devices. the 20th Annual Network andDistributed System Security Symposium (NDSS),Feb. 2013.

[12] Wang W, Li Z, Owens R, et al. Secure andefficient access to outsourced data. in: Proceedingsof the 2009 ACM workshop on Cloud computingsecurity. Chicago, USA: ACM pp. 55-66, 2009.

[13] Maheshwari U, Vingralek R, Shapiro W. Howto build a trusted database system on untrustedstorage. in: Proceedings of the 4th conference onSymposium on Operating System Design &Implementation-Volume 4. USENIX Association,pp. 10-12, 2000.

[14] Kan Yang, XiaohuaJia, KuiRen: Attributebasedfine-grained access control with efficientrevocation in cloud storage systems. ASIACCS2013, pp. 523-528, 2013.

[15] Crampton J, Martin K, Wild P. On keyassignment for hierarchical access control. in:Computer Security Foundations Workshop. IEEEpress, pp. 14-111, 2006.

[16] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[17] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[18] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DAC- MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensicsand Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[19] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

ABOUT AUTHORS:

T. Neha Singh is currently working as an Assistant Professor in Computer Science & Engineering Department, Malla Reddy Institute of Technology & Science, Secunderabad.

K. Mamatha is currently working as an Assistant Professor in Computer Science & Engineering Department, Malla Reddy Institute of Technology & Science, Secunderabad.