International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing using A Key Management Protocol

Pradnya V kothawade[1],Priyanka More[2], Sunil S Mirashe[3], Priyanka A Salunke[4], Ritesh S Methalkar[5], Neha V Rawandalekar[6]

[1,2,3,4,5,6]*Genba Sopanrao Moze College Of Engineering, Pune (India)*

ABSTRACT

Ciphertext policy attribute-based writing (CP-ABE) may even be a promising branch of knowledge technique for fine-grained access management of outsourced data within the cloud. However, some drawbacks of key management hinder the recognition of its application. One balk in imperative would like of resolution is that the key legal document disadvantage. we've associate inclination to purpose that front-end devices of shoppers like smart phones typically have restricted privacy protection, thus if personal keys unit entirely management by them, shoppers risk key exposure that's hardly noticed however inherently existed in previous analysis. moreover, monumental shopper decoding overhead limits the good use of ABE. throughout this work, we've associate inclination to propose a cooperative key management protocol in CP-ABE (CKM-CP-ABE).

Keywords:-Cloud data sharing, CP-ABE, Key management,Security, efficiency.

I.INTRODUCTION

With cost-effectiveness enhancements in procedure technology and huge scale networks, sharing information with others becomes correspondingly additional convenient. to boot, digital resources are additional just obtained via cloud computing and storage. Since cloud information sharing needs off-premises infrastructure that some organizations put together command, remote storage are somehow threatening privacy of information owners. Therefore, imposing the protection of non-public, confidential associated sensitive information keep within the cloud is unbelievably crucial The synchronic participation of associate degree outsize vary of users needs fine grained access management for information sharing. Attribute-based secret writing (ABE) might even be a promising branch of knowledge primitive that features a stimulating resolution to secure and versatile information sharing. ABE has associate inherent one-to-many property ,which means one key will decipher totally completely totally different |completely different} cipher texts or different keys will decipher identical ciphertext[2]. There unit of measure 2 sorts of ABE, referred to as ciphertext policy ABE (CP-ABE) and key policy ABE (KP-ABE). For CP-ABE, the access policy is embedded into a ciphertext and put together the attribute set is embedded into a non-public key. For KP-ABE, the access policy is embedded into a non-public key and put together the attribute set is embedded into a ciphertext. CP-ABE permits data owners to stipulate their own access policy. Anyone World Health Organization has got to get data[1][3]must initial match the

access policy attribute set. because of this property, CP-ABE is style of acceptable for the event of secure, fine-grained access management for cloud data sharing ABE comes in 2 flavors referred to as key-policy ABE (KP-ABE) and ciphertext-policy .ABE. In KP-ABE, attributes area unit accustomed describe the encrypted data and policies area unit designed into users keys; whereas in CP-ABE, the attributes area unit accustomed describe a users papers, associated associate degree code or determines a policy on World Health Organization can rewrite the data[2][3][4]

II. EXISTING SYSTEM

Ciphertext policy attribute-based secret writing (CP-ABE) is also a promising of information} technique for fine-grained access management of outsourced data within the cloud. However, some drawbacks of key management hinder the recognition of its application. One disadvantage in pressing want of resolution is that the key papers balk.[7] we've AN inclination to purpose that front-end devices of purchasers like smartphones usually have restricted privacy protection, thus if personal keys unit of measure entirely management by them, purchasers risk key exposure that's hardly detected however inherently existed in previous analysis. what's additional, monumental consumer writing overhead limits the sensible use of Attribute primarily based secret writing. previous schemes of key management in attribute-based info sharing system primarily focuses on key update, proxy re-encryption and outsourced writing. Some analysis incontestable untrusted key authority could result in key papers balk and provided corresponding solutions[5].

Existing System Disadvantages:

1. One drawback is the key escrow problem.
2. key authority must be completely trustworthy, as it can decrypt all the cipher text using a generated private key without permission of its owner.

III.OBJECTIVE

1. Attribute based data sharing.
2. Data stored in encrypted format to improve privacy.
3. Collaborative key management for resolving key escrow problem.
4. Well defined access structure for improve security.

IV.PROPOSED SYSTEM

propose awfully distinctive cooperative key management protocol in ciphertext policy attribute-based secret writing(CKM-CP-ABE) attending to enhance security and potency of key management in cloud data sharing system. the foremost contributions unit of activity summarized. we tend to introduce attribute teams to make the non-public key update rule. a singular attribute cluster secret is allotted to every attribute cluster that contains purchasers World Health Organization share the same attribute. Via modification attribute cluster key, a fine-grained and immediate attribute revocation is provided. we have a tendency to tend to tend to purpose that not alone key legal document disadvantage however conjointly key exposure is threatening the confidentiality of

personal keys, that is hardly detected in previous analysis. Compared to previous key management protocols for attribute-based data sharing system in cloud, our planned protocol effectively addresses each 2 issues by its cooperative key management.[9][10] Finally, we offer proof of security for the planned protocol. The cooperative mechanism helps markedly prune consumer decoding overhead by using a decoding server to execute most of decoding whereas leave no data about data to that.

Proposed System Advantages:

1. In proposed system, novel collaborative protocol is presented. With help of interaction among the key authority, a cloud server and client who tends to access data, We resolve the key escrow problem.
2. Resolve Key exposure problem.

V.ALGORITHMS

Algorithm 1:AES Algorithm

Algorithm Steps

Step 1: Start

Step 2: Derive the set of round keys from the cipher key.

Step 3: Initialize the state array with the block data (plaintext). .

Step 4:Add the initial round key to the starting state array.

Step 5: Add the initial round key to the starting state array.

Step 6:Perform the tenth and final round of state manipulation..

Step 7: Copy the final state array out as the encrypted data (cipher text).

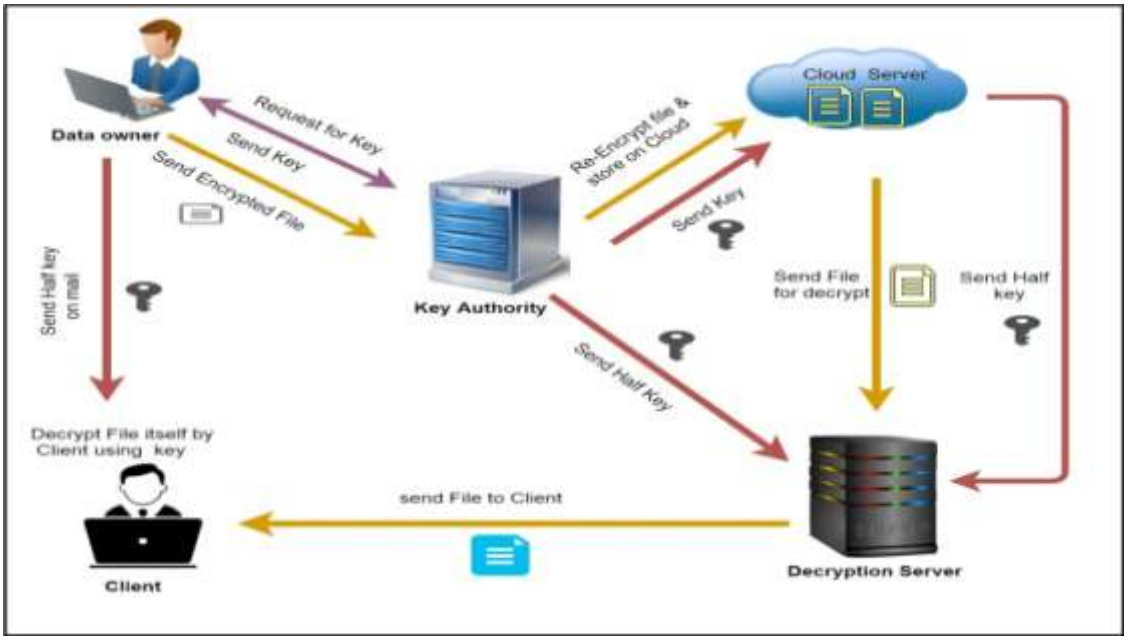

fig:1:Architecture diagram

System Requirement and Specification

Hardware resources required

1. Processor : Pentium –IV
2. Speed : 1.1 GHz
3. RAM : 256 MB(min)
4. Hard Disk : 20 GB
5. Key Board : Standard Windows Keyboard
6. Mouse : Two or Three Button Mouse
7. Monitor : SVGA

Software resources required

1. Operating System: Windows 07/08/Above
2. Programming Language:JAVA/J2EE/XML
3. Database : MY SQL

PROJECT RESULT

fig 2:snapshot(upload data)

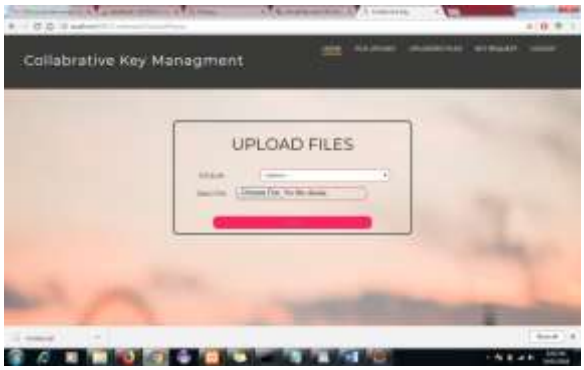

fig3:snapshot: upload files

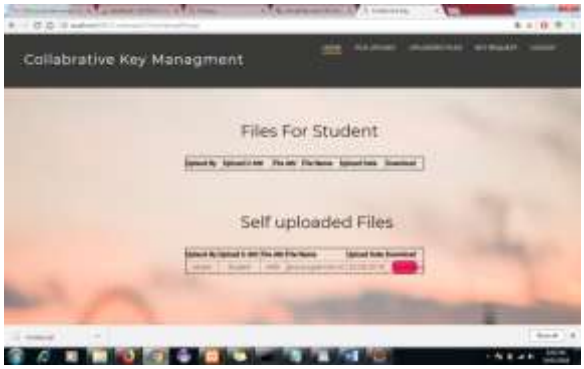

fig4:snapshot: check the files.

VI.CONCLUSION AND FUTURE SCOPE

Secure key management is guaranteed without adding any extra physical infrastructure. The projected cooperative mechanism fully addresses not only key instrument downside but collectively a worse downside referred to as key exposure that previous analysis hardly noticed .in the meantime it helps to optimize clients' user experience since only a tiny low amount of responsibility is taken by them for secret writing. Thus, the projected theme performs higher in cloud data sharing system serving giant performance-restrained front-end device.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EuroCrypt, 2005, pp. 457-473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc.ACM CCS, 2006, pp. 89-98.

[3] L. Cheung, and C. Newport, "Provably secure ciphertext policy ABE," inProc. ACM CCS, 2007, pp. 456-465.

[4] J. Hur, and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214-1221, 2011.

[5] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive,efficient, and provably secure realization," in Proc. Public KeyCryptography, 2011, pp. 53-70.

[6] M. Green, S. Hohnberger, and B. Waters, "Outsourcing the decryption ofABEciphertext," in Proc. USENIX Secur. Symp., 2011, pp. 34.

[7] J. Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policyattribute-based encryption," in Proc. IEEE Symp.Secur. Privacy, 2007,pp. 321-334.

[8] P. P. Chandar, D. Mutkurman, and M. Rathinrai, "Hierarchical attributebased proxy reencryption access control in cloud computing," in Proc.ICCPCT, 2014, pp. 1565-1570.

[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryptionwith verifiable outsourced decryption," IEEE Trans. Inf. Forens.Security, vol. 8, no. 8, pp. 1343-1354, 2013.

[10] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-basedencryption with verifiable outsourced decryption," IEEE Trans. Inf.Forens. Security, vol. 10, no. 10, pp. 2119-2130, 2015.