Scientific Journal of Impact Factor (SJIF): 5.71

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

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

SECURELY DATA SHARING WITH TIME SERVER CP-ABE IN CLOUD COMPUTING USING KEY MANAGEMENT PROTOCOL.

Rakshit Raj, Shivam Tripathi, Nidhi Tammewar, Vikash Kumar

Sinhgad Institute of Technology, Lonavala, India

Abstract:- *Ciphertext-policy attribute-based coding (CP-ABE) may be a promising cryptological technique for fine-grained access management of outsourced knowledge within the cloud. However, some drawbacks of key management hinder the recognition of its application. One downside in imperative want of resolution is that the key written agreement drawback. we have a tendency to indicate that front-end devices of shoppers like sensible phones typically have restricted privacy protection, therefore if personal keys are entirely controlled by them, shoppers risk key exposure that's hardly noticed however inherently existed in a previous analysis. moreover, monumental consumer decoding overhead limits the sensible use of ABE. during this work, we have a tendency to propose a cooperative key management protocol in CP-ABE (CKM-CP-ABE). Our construction realizes distributed generation, issue, and storage of personal keys while not adding any additional infrastructure. A fine-grained and immediate attribute revocation is provided for a key update. The projected cooperative mechanism effectively solves not solely key written agreement drawback however conjointly key exposure. Meanwhile, it helps markedly scale back consumer decoding overhead. A comparison with different representative CP-ABE themes demonstrates that our scheme has somewhat higher performance in terms of cloud-based outsourced knowledge sharing on mobile devices. Finally, we offer proof of security for the projected protocol.*

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

I. INTRODUCTION

BIG knowledge may be a high volume, and/or high rate, high selection information quality, which needs new kinds of process to modify increased deciding, insight discovery, and method optimization [1]. Because of its complexness and enormous volume, managing huge knowledge victimisation handy direction tools is difficult. a good answer is to source the info to a cloud server that has the capabilities of storing huge knowledge and process users' access requests in associate economical manner. for instance in ehealth applications, the ordination info ought to be firmly stored in associate e-health cloud as one sequenced human ordination is around one hundred forty gigabytes in size [2], [3]. However, once a knowledge owner outsources its knowledge to a cloud, sensitive info might be disclosed as a result of the cloud server isn't trusted; thus typically the ciphertext of the info is hold on within the may. But how to update the ciphertext hold on during a cloud once a brand new access policy is selected by the info owner and the way to verify the legitimacy of a user World Health Organization intends to access the info ar still of nice considerations. Most existing approaches for securing the outsourced huge knowledge in clouds ar supported either attributed-based coding (ABE) or secret sharing. ABE primarily based approaches give the flexibility for a knowledge owner to predefine the set of users World Health Organization are eligible for accessing the info however they suffer from the high complexity of expeditiously change the access policy and ciphertext. Secret sharing [11]–[17] mechanisms permit a secret to be shared and reconstructed by bound range of cooperative users however they typically use uneven public key cryptograph like RSA for users' legitimacy verification, that incur high process overhead. Moreover, it's conjointly a difficult issue to dynamically and expeditiously update the access policies in keeping with the new requirements of the info homeowners secretly sharing approaches. As {a knowledge an information} owner generally doesn't backup its data regionally when outsourcing the info to a cloud, it cannot simply manage the info stored within the cloud. Besides, as a lot of and a lot of firms and organizations ar victimization clouds to store their knowledge, it becomes a lot of challenging and demanding to modify the difficulty of access policy update for enhancing security and coping with the dynamism caused by the users' be a part of and leave activities. To the simplest of our knowledge, policy update for outsourced huge knowledge storage in clouds has ne'er been thought-about by the present analysis.

II. EXISTING SYSTEM

Ciphertext policy attribute-based secret writing (CP-ABE) could be a promising scientific discipline technique for fine-grained access management of outsourced knowledge 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 written agreement downside. we have a tendency to indicate that front-end devices of purchasers like good phones usually have restricted

privacy protection, therefore if non-public keys square measure entirely control by them, purchasers risk key exposure that's hardly noticed however inherently existed in previous analysis. what is more, monumental consumer coding overhead limits the sensible use of Attribute primarily based secret writing. previous schemes of key management in attribute-based knowledge sharing system primarily focuses on key update, proxy re-encryption and outsourced coding. Some analysis incontestable untrusted key authority could result in key written agreement downside and provided corresponding solutions.

Existing System Disadvantages:

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

IV 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.

III. PROPOSED SYSTEM

We propose a completely unique cooperative key management protocol in ciphertext policy attribute-based encryption (CKM-CP-ABE) getting to enhance security and potency of key management in cloud knowledge sharing system. the most contributions area unit summarizedwe tend to introduce attribute teams to make the non-public key update algorithmic program. a singular attribute cluster secret is allotted to every attribute cluster that contains purchasers World Health Organization share the same attribute. Via change attribute cluster key, a fine-grained and immediate attribute revocation is provided. we tend to indicate that not solely key written agreement drawback 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 knowledge sharing system in cloud, our planned protocol effectively addresses each 2 issues by its cooperative key management. Finally, we offer proof of security for the planned protocol. The cooperative mechanism helps markedly cut back consumer decoding overhead by using a decoding server to execute most of decoding whereas leave no information regarding 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.

IV. ALGORTHMS

Algorithm 1: AES Algorithm
Alogrithm 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 (ciphertext).

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

V. SIMMULATION RESULTS

The simulation studies involve:

Data owner:

I. Registration (id, name, email, contact, address)
II. Data owner (profile, send request for key Authority, upload file, download file, logout)
III. Login
IV. Send request to key Authority to key for file upload
V. Key authority send half part of key to data owner .using this key, data owner encrypt file and send initial encrypted file to Key authority using AES Algorithm.
VI. Download self uploaded file.
VII. Logout.

Key Authority

I. Registration.
II. Key Authority (view Request, Display files, logout)
III. Login
IV. View request of data owner for key.
V. Key is divided into three parts one for data owner, 2 nd for cloud and 3 rd for client.
VI. Receive initial encrypted file from data owner and again Re-Encrypt file using own key and
VII. Upload over cloud.
VIII. Logout.

Cloud admin.

Cloud Admin (profile, view files, view request, logout)
I. Registration (id ,name ,mail ,contact ,address)
II. Login
III. View all uploaded file by key authority.
IV. Display all information of data owners, clients and files
V. Send encrypted file to decryption server for decryption
VI. Logout

Decryption server

(View files for decrypt, Logout)
I. Login View files request for decrypt
II. For decryption of file, it requires two parts of key, one from cloud and 2nd from key authority.
III. After receiving keys, decryption server partially decrypts the file and sends to the authorized client.
IV. Logout

Client

I. Registration
II. Login
III. View key on mail and use for file decryption.

IV. Receive file from decryption server and properly decrypt file using key that is provided by key authority.
V. Download file
VI. Logout

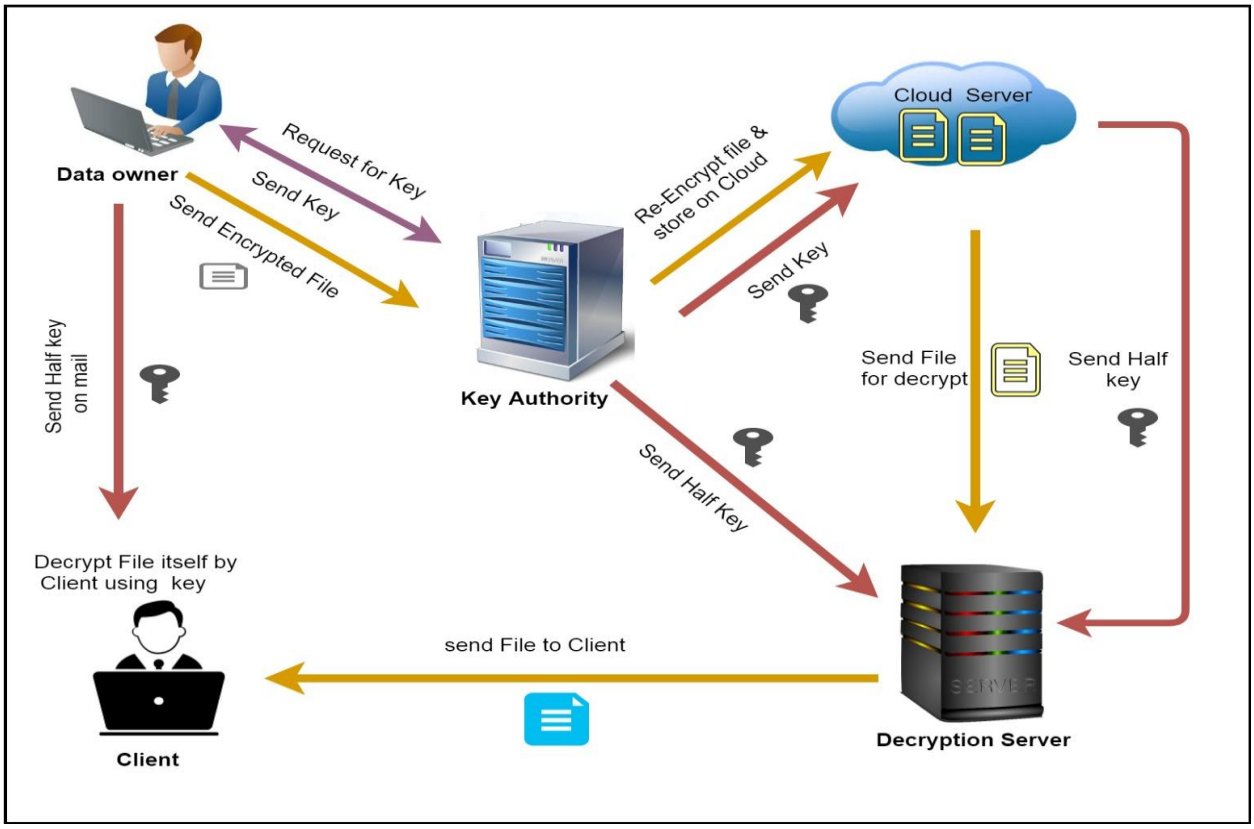

Fig.1 Showing the working of the System.

VI. CONCLUSION AND FUTURE SCOPE

The proposed collaborative mechanism perfectly addresses not only key escrow problem but also a research hardly noticed. Meanwhile it helps to optimize clients' user experience since only a small amount of responsibility is taken by them for decryption. Thus the proposed scheme perform better in cloud data sharing system serving massive performance

VII. ACKNOWLEDGEMENTS

We would like to thank the researchers as well as publishers for making their resources available and our guide prof. V.N. Dhawas for their guidance and suggestions.

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 ofABE ciphertext," 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.

