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 06, June -2018

EFFICIENT KEY MANAGEMENT PROTOCOL FOR DATA SHARING IN CLOUD.

Satwik Deshmukh 1st, Vijay Panhalkar2nd, Suraj Supekar3rd , Shubham Jadhav4th
Prof. Manisha Darak 5th

Siddhant Collage of Engineering, Sudumbre

Abstract:- *Ciphertext policy attribute-based cryptography (CP-ABE) is additionally a promising science technique for fine-grained access management of outsourced info at intervals the cloud. However, some drawbacks of key management hinder the recognition of its application. One recoil in imperative want of resolution is that the key legal instrument draw back. we have got AN inclination to purpose that front-end devices of shoppers like wise phones sometimes have restricted privacy protection, therefore if personal keys unit of measurement entirely management by them, shoppers risk key exposure that's hardly detected however inherently existed in previous analysis. moreover, monumental consumer cryptography overhead limits the wise use of ABE. throughout this work, we have got AN inclination to propose a cooperative key management protocol in CP-ABE (CKM-CP-ABE). Our construction realizes distributed generation, issue and storage of personal keys whereas not adding any additional infrastructure. A fine-grained and immediate attribute revocation is provided for key update. The projected cooperative mechanism effectively solves not entirely key legal instrument draw back however put together key exposure. Meanwhile, it helps markedly shrink consumer cryptography overhead. A comparison with utterly totally different representative CP-ABE themes demonstrates that our theme has somewhat higher performance in terms of cloud-based outsourced info 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

With cost-effectiveness enhancements in procedure technology and large scale networks, sharing data with others becomes correspondingly further convenient. additionally, digital resources ar further merely obtained via cloud computing and storage. Since cloud data sharing wants off-premises infrastructure that some organizations jointly command, remote storage ar somehow threatening privacy of data homeowners. Therefore, imposing the protection of personal, confidential associated sensitive data keep inside the cloud is extremely crucial The parallel participation of an oversized vary of users wants fine grained access management for data sharing. Attribute-based secret writing (ABE) is also a promising cryptographic primitive that gives a remarkable resolution to secure and versatile data sharing. ABE has associate inherent one-to-many property,which means one key can decipher fully completely different|completely different} ciphertexts or different keys can decipher identical ciphertext. There unit a pair of styles of ABE, called ciphertext policy ABE (CP-ABE) and key policy ABE (KP-ABE). For CP-ABE, the access policy is embedded into a ciphertext and additionally the attribute set is embedded into a private key. For KP-ABE, the access policy is embedded into a private key and additionally the attribute set is embedded into a ciphertext. CP-ABE permits data homeowners to stipulate their own access policy. Anyone World Health Organization must get data
must initial match the access policy attribute set. thanks to this property, CP-ABE is style of applicable for the event of secure, fine-grained access management for cloud data sharing ABE comes in a pair of flavors called key-policy ABE (KP-ABE) and ciphertext-policy .ABE. In KP-ABE, attributes area unit accustomed describe the encrypted information and policies area unit engineered into users keys; whereas in CP-ABE, the attributes area unit accustomed describe a users document, associated an write in code or determines a policy on WHO will rewrite the information.

II LITERATURE SURVEY

Paper1: Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems.
In this paper, we tend to propose associate degree access management mechanism victimization ciphertext-policy attribute-primarily based encoding to enforce access management policies with economical attribute and user revocation capability. The fine-grained access management may be achieved by twin encoding mechanism that takes advantage of the attribute-based encoding and selective cluster key distribution in every attribute cluster. we tend to demonstrate a way to apply the planned mechanism to firmly manage the outsourced knowledge. The analysis results indicate that the planned theme is

economical and secure within the knowledge outsourcing systems. ABE comes in 2 flavors known as key-policy ABE (KP-ABE) and ciphertext-policy ABE.

Paper2: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
We develop a brand new cryptosystem for ¯ne-grained sharing of encrypted information that we tend to decision Key-Policy Attribute-Based cryptography (KP-ABE). In our cryptosystem, ciphertexts area unit labeled with sets of attributes and personal keys area unit related to access structures that management that ciphertexts a user is in a position to rewrite. we tend to demonstrate the relevance of our construction to sharing of audit-log data and broadcast cryptography. Our construction supports delegation of personal keys that subsumes hierarchical Identity-Based cryptography (HIBE)..In our system, Fine-grained access management systems facilitate granting access rights to a collection of users and permit exibility in specifying the access rights of individual users. many techniques area unit legendary for implementing ¯ne grained access management.

Paper3: Ciphertext-Policy Attribute-Based Encryption: An Expressive, E_cient, and Provably Secure Realization
In our most effcient system, ciphertext size, encryption, and secret writing time scales linearly with the quality of the access formula. the sole previous work to attain these parameters was restricted to a signal within the generic cluster model. we tend to gift 3 constructions among our framework. Our system is verified by selection secure underneath a assumption that we tend to decision the decisional Parallel additive Diffle -Hellman Exponent (PBDHE) assumption which may be viewed as a generalization of the BDHE assumption.

Paper4: Fuzzy Identity-Based Encryption.
A Fuzzy IBE theme are often applied to alter encoding victimization biometric inputs as identities; the error-tolerance property of a Fuzzy IBE theme is exactly what permits for the utilization of biometric identities, that inherently can have some noise when they're sampled. to boot, we have a tendency to show that Fuzzy-IBE are often used for a sort of application that we have a tendency to term “attribute-based encryption”. during this paper we have a tendency to gift 2 constructions of Fuzzy IBE schemes. Our constructions are often viewed as associate Identity-Based encoding of a message underneath many attributes that compose a (fuzzy) identity. Our IBE schemes ar each error-tolerant and secure against collusion attacks. to boot, our basic construction doesn't use random oracles. we have a tendency to prove the protection of our schemes underneath the Selective-ID security model.

Paper5: Provably Secure Ciphertext Policy ABE In this paper, we study CP-ABE schemes in which access structures are AND gates on positive and negative attributes. Our basic scheme is proven to be chosen plaintext (CPA) secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. We then apply the Canetti-Halevi-
Katz technique to obtain a chosen ciphertext (CCA) secure extension using one-time signatures. The security proof is a reduction to the DBDH assumption and the strong existential unforgeability of the signature primitive.

III EXISTING SYSTEM

Ciphertext policy attribute-based secret writing (CP-ABE) can be a promising subject area} technique for fine-grained access management of outsourced knowledge at intervals the cloud. However, some drawbacks of key management hinder the popularity of its application. One disadvantage in pressing need of resolution is that the key official document draw back. we've a bent to point that front-end devices of purchasers like sensible phones typically have restricted privacy protection, thus if personal keys unit of measurement entirely management by them, purchasers risk key exposure that is hardly noticed but inherently existed in previous analysis. what's a lot of, monumental client committal to writing overhead limits the smart use of Attribute based secret writing. previous schemes of key management in attribute-based information sharing system primarily focuses on key update, proxy re-encryption and outsourced committal to writing. Some analysis incontestable untrusted key authority may end in key official document draw back 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.

V PROPOSED SYSTEM

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.

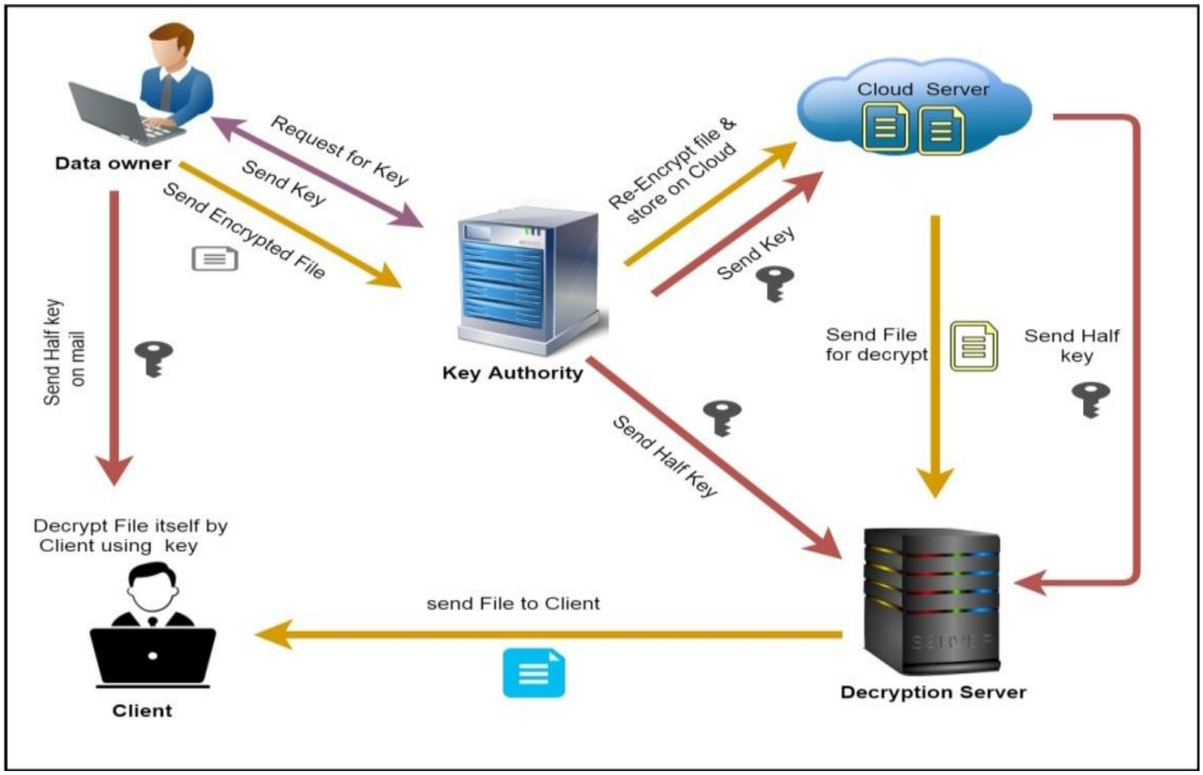
Proposed System Advantages:

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.

V ALGORITHMS

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

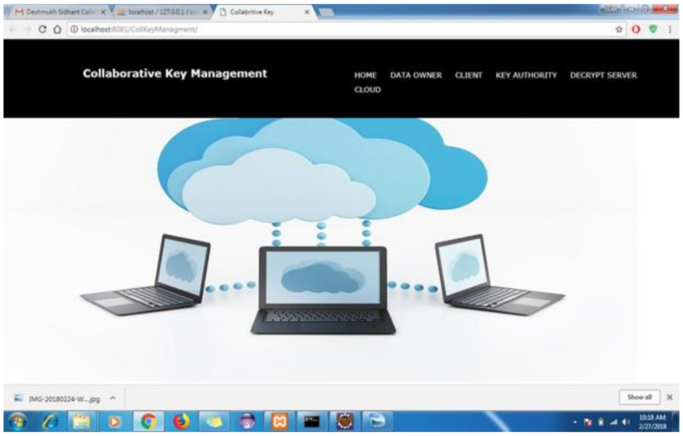
Software resources required

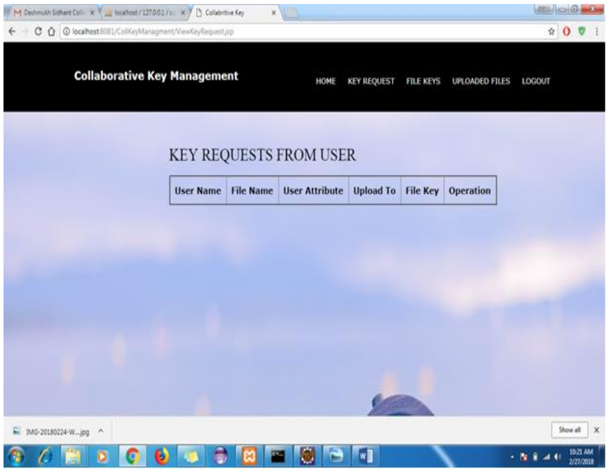
1.	Operating System	:	Windows 07/08/Above
2.	Programming Language	:	JAVA/J2EE/XML
3.	Database	:	MY SQL

VI CONCLUSION AND FUTURE SCOPE

The planned cooperative mechanism absolutely addresses not solely key written agreement downside however conjointly a worse downside known as key exposure that previous analysis hardly noticed . meantime it helps to optimize clients' user expertise since solely atiny low quantity of responsibility is taken by them for cryptography. Thus, the planned theme performs higher in cloud knowledge sharing system serving large performance-restrained front-end devices with relevance either security or potency

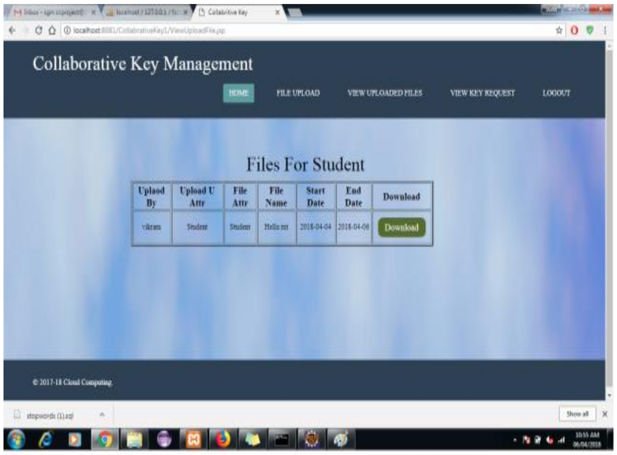
RESULT





KEY REQUESTS FROM USER

User Name	File Name	User Attribute	Upload To	File Key	Operation



Files For Student

Uplaod By	Upload U Attr	File Attr	File Name	Start Date	End Date	Download
vikram	Student	Student	Hello mr	2018-04-04	2018-04-08	Download

© 2017-18 Cloud Computing.

VII ACKNOWLEDGEMENTS

This Work is supported by Prof.Subhash Patel (Siddhant College of Engineering)

VIII 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.