A Novel Capable Attribute -Based Encription Method for Shared Cloud Data Files

Sajjala Satee Devi & A.Sandhya Rani

[1]M.Tech Student, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA , A.P, India

[2]Assistant Professor & HOD, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA, A.P, India

Abstract: *With the growing status of cloud computing, firms and data owners begins to outsource their primary data to the general public cloud for decreased management price and ease of access. Encryption helps to shield user data confidentiality, it makes tricky to perform comfy undeniable textual content search over the encrypted data Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the flexibility of entry manage mechanisms. There are two complementary types of attribute headquartered encryption. One is key-policy attribute-based encryption (KP-ABE) and the opposite is cipher text-policy attribute-based encryption (CPABE). In a KP-ABE process, the decision of access coverage is made by the important thing distributor instead of the encipherer, which limits the practicability and value for the system in useful functions. On the contrary, in a CP-ABE system, every cipher textual content is associated with an entry constitution, and each confidential secret is labeled with a collection of descriptive attributes.*

Keywords: Cloud storage, outsourcing computing, cloud storage auditing, key update, verifiability.

1. Introduction

In any case, if an administration is helpless against assaults or disappointments, it would convey hopeless misfortunes to the customers in light of the fact that their information or documents are put away in a dubious stockpiling pool outside the ventures. These security dangers originate from the accompanying reasons: it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third-party auditor (TPA)

who has expertise and capable to audit the outsourced data when needed. Public audit ability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data In this way, it is fundamental for CSP to offer a productive review administration to check the respectability and accessibility of put away data.It is attractive that cloud just engages confirmation ask for from a solitary assigned gathering. To completely guarantee the information respectability and spare the cloud client's calculation assets and in addition online weight, it is of basic significance to empower open examining administration for cloud information stockpiling, with the goal that clients may depend on an autonomous outsider inspector (TPA) who has skill and proficient to review the outsourced information when required. Open review capacity permits an outer gathering, notwithstanding the client himself, to confirm the accuracy of remotely put away information This extreme disadvantage extraordinarily influences the security of these conventions in distributed computing. It is an endeavor to demonstrate the security by applying different systems and legitimize the execution of proposed plans through solid trials and examinations. It is our endeavor to give security to the cloud by just basically utilizing Kerberos frameworks for open review capacity. In

particular, proposed plot accomplishes group examining where various assigned inspecting undertakings from various

clients can be performed at the same time by the TPA in a protection safeguarding way

II. LITERATURE SURVEY

ATTRIBUTE BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA:

As extra sensitive data is shared and stored on the web, there will be a need to encrypt data stored at these websites. One drawback is that it can be selectively shared only at a rough-grained level (i.e., giving a different party your exclusive key). We develop a new cryptosystem for fine-grained sharing of encrypted information that we call Key-policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with units of attributes and confidential keys are associated with entry constructions that control which ciphertexts a consumer is capable to decrypt. We display the applicability of our building to sharing of audit-log know-how and broadcast encryption. Our building helps delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). It's the first decentralized ABE scheme with privacy-keeping founded on regular complexity assumptions.

A PRACTICAL PUBLIC KEY CRYPTOSYSTEM PROVABLY SECURE AGAINST CHOSEN CIPHERTEXT ATTACK:

This paper presents a novel framework for development of hybrid encryption schemes secure against chosen ciphertext assault. Our new framework yields new and extra effective CCA-secure schemes, and supplies insightful explanations about present schemes that don't match into the earlier frameworks. This could influence in finding future upgrades. Furthermore, it enables immediate conversion from a category of threshold public-key encryption to a hybrid one without considerable overhead, which is not achievable within the previous strategies.

A NEW PARADIGM OF HYBIRD ENCRYPTION SCHEME:

In this paper, we show that a key encapsulation mechanism (KEM) does no longer need to be IND-CCA secure within the development of hybrid encryption schemes, as used to be earlier believed. That is, we present a extra efficient hybrid encryption scheme by way of making use of a KEM which is not always IND-CCA secure. However, our scheme is secure within the experience of IND-CCA below the DDH assumption in the common mannequin. This outcomes is additional generalized to universal two projective hash families.

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which drastically enhances the flexibility of access control mechanisms. Due to the excessive expressiveness of ABE insurance policies, the computational complexities of ABE key-issuing and decryption have become prohibitively excessive. Despite that the prevailing Outsourced ABE solutions are able to dump some intensive computing duties to a 3rd get together, the verifiability of outcome again from the 1/3 occasion has yet to be addressed. Aiming at tackling the challenge above, we advise a brand new cozy Outsourced ABE procedure, which supports each secure outsourced key-issuing and decryption. Our new method offloads all entry coverage and attribute related operations in the key-issuing system or decryption to a Key Generation Service Provider and a Decryption Service Provider (DSP), respectively, leaving only a constant number of straightforward operations for the attribute authority and eligible customers to participate in the neighborhood. In addition, for the first time, we endorse an outsourced ABE construction which presents examine capability of the outsourced computation results in an effective approach..

OUTSOURCING THE DECRYPTING OF ABE CIPHERTEXTS:

Attribute-Based Encryption (ABE) is a brand new imaginative and prescient for public key encryption that makes it possible for users to encrypt and decrypt messages headquartered on person attributes. For instance, a consumer can create a ciphertext that can be decrypted best with the aid of different users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for a lot of cloud storage and computing functions. However, one of the predominant efficiency drawbacks of ABE is that the dimensions of the ciphertext and the time required to decrypt it grows with the complexity of the entry system. On this work, we recommend a brand new paradigm for ABE that mostly eliminates this overhead for users. Think that ABE ciphertexts are saved in the cloud. We show how a user can provide the cloud with a single transformation key that makes it possible for the cloud to translate any ABE ciphertext satisfied through that consumer's attributes right into a (steady-measurement) El Gamal-form ciphertext, without the cloud being ready to read any part of the consumer's messages. To exactly define and reveal the benefits of this procedure, we furnish new protection definitions for each CPA and replayable CCA safety with outsourcing, several new constructions, an implementation of our algorithms and designated performance measurements. In a traditional configuration, the consumer saves significantly on both bandwidth and decryption time, without growing the quantity of transmissions.

III. EXISTING SYSTEM:

- ❖ Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang *et al.* proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE.
- ❖ Wan *et al.* proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A ciphertext policy hierarchical ABE scheme with short ciphertext is also studied.
- ❖ In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.

DISADVANTAGES OF EXISTING SYSTEM:

- In Existing System time and cost for encryption is high.
- No any special multiple hierarchical files are used. Decryption system time and computation cost are very high

IV.PROPOSED WORK

In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.

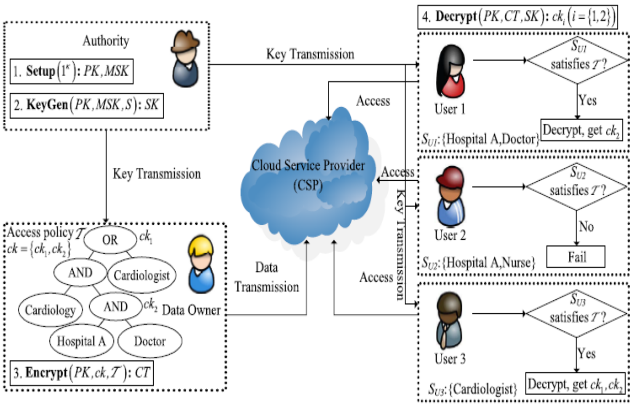
The contributions of our scheme are three aspects.

Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure.

Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption..

SYSTEM ARCHITECTURE


Authority
1. **Setup**(1^κ): PK, MSK
2. **KeyGen**(PK, MSK, S): SK
Key Transmission
Key Transmission
Access policy $\mathcal{T}$
$ck = \{ck_1, ck_2\}$
OR
ck_1
AND
Cardiologist
Cardiology
AND
ck_2
Data Owner
Hospital A
Doctor
3. **Encrypt**$(PK, ck, \mathcal{T})$: CT
Data Transmission
Cloud Service Provider (CSP)
Access
Access
Access
Key Transmission
4. **Decrypt**(PK, CT, SK): ck_i $(i = \{1,2\})$
User 1
S_{U1} satisfies $\mathcal{T}$?
Yes
Decrypt, get ck_2
S_{U1}:{Hospital A,Doctor}
User 2
S_{U2} satisfies $\mathcal{T}$?
No
Fail
S_{U2}:{Hospital A,Nurse}
User 3
S_{U3} satisfies $\mathcal{T}$?
Yes
Decrypt, get ck_1, ck_2
S_{U3}:{Cardiologist}

V. IMPLEMENTATION

1. Attribute Authority:

Authority will have to offer the key, as per the consumer's key request. Every customers request can must be raised to authority to set off access key on mail. There are 2 complementary forms of attribute-headquartered secret writing. One is key-policy attribute-based Encryption (KP-ABE) and the alternative is ciphertext-policy attribute-based encryption (CPABE). In a KP-ABE approach, the selection of entry coverage is created by means of the key distributor instead than the encipherer, which limits the usefulness and usefulness for the system in sensible functions.

2. Cloud Server:

Cloud server may have the entry to documents that rectangular measure uploaded through the understanding proprietor Cloud server wishes to decipher the records offered underneath their permission.

In addition expertise user can must decipher the data to entry the preliminary text through offering the character key. File has been decrypted efficaciously and supplied for shopper.

3.Data owner:

Data owner can have to register initio to result in access to the profile. Data owner can transfer the file to the cloud server in the encrypted format. Random encryption key new release is going down whereas uploading the file to the cloud. Encrypted file will be hold on the cloud.

4. Data Consumer:

Data consumer may also be initio lift for the key to the Authority to verify and decipher the enter the cloud. Data consumer will access the file mainly established on the important thing received from mail identification. As per the key bought the customer will affirm and decipher the info from the cloud.

VI. CONCLUSION

In this paper, we study on how to outsource key updates for cloud storage auditing with key-exposure resilience. We propose the first cloud storage auditing protocol with verifiable outsourcing of key updates. In this protocol, key updates are outsourced to the TPA and are transparent for the client. In addition, the TPA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. We give the formal security proof and the performance simulation of the proposed scheme.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, ”Above the Clouds: A Berkeley View of Cloud Computing,” University of California, Berkeley, Technical Report, no. UCB/EECS-2009-28, 2009.

[2] M. Green, S. Hohenberger and B. Waters, ”Outsourcing the Decryption of ABE Ciphertexts,” in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[3] J. Lai, R. H. Deng, C. Guan and J. Weng, ”Attribute-Based Encryption with Verifiable Outsourced Decryption,” in Proc. IEEE Transactions on information forensics and security, vol. 8, NO. 8, pp.1343-1354, 2013.

[4] A. Lewko and B. Waters, ”Decentralizing Attribute-Based Encryption,” in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[5] B. Waters, ”Ciphertext-Policy Attribute-Based Encryption: an Expressive, Enficient, and Provably Secure Realization,” in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[6] B. Parno, M. Raykova and V. Vaikuntanathan, ”How to Delegate and Verify in Public: verifiable computation from attribute-based encryption,” in Proc. TCC, pp.422-439, Springer-Verlag Berlin, Heidelberg, 2012.

[7] S. Yamada, N. Attrapadung and B. Santoso, ”Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication,” in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.

[8] J. Han, W. Susilo, Y. Mu and J. Yan, ”Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption,” in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai and B. Waters, ”Attribute-Based Encryption for Circuits from Multilinear Maps,” in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin, Heidelberg, 2013.

[10] S. Gorbunov, V. Vaikuntanathan and H. Wee, ”Attribute-Based Encryption for Circuits,” in Proc. STOC, pp.545-554, ACM New York, NY, USA, 2013.