Journal of Engineering Sciences

Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

A Scalable and Efficient User Revocation Mechanism Using Attribute-Based Hybrid Encryption in Cloud Computing

KATAKAM SRINIVASA RAO, Associate Professor
M.S.R LAKSHMI REDDY, Associate Professor
DEPARTMENT OF CSE
CMR INSTITUTE OF TECHNOLOGY, HYDERABAD

Abstract: With the growing popularity of cloud computing, organizations and data owners starts to outsource their important data to the public cloud for reduced management cost and ease of access. Encryption helps to protect user data confidentiality, it makes difficult to perform secure plain text search over the encrypted data. For secure access of the data, data owners can go for the encryption that is based on the attributes to encrypt the data that has been stored in the server. A user has authority to access the data if a user has a certain set of attributes. In the cloud, for getting access control and maintaining data secure and for the exactness of the secure computing results, the data owner has to kept attribute-based security to encrypt the stored data. Since during the delegation, the cloud servers have tampered or replaced the cipher-text and change a forged computing result with malicious intent. They may also cheat the authorized users by responding them that they are unauthorized for the cost saving purpose. Many times, during the encryption, the control access attribute policies may not easy enough as well. In this paper we present a system for maintain complex access control on encrypted data that we call scalable and efficient user revocation mechanism using attribute-based encryption with verifiable delegation computation. By using our techniques encrypted data can be kept data confidential. Further Moreover, our methods are highly secured against collusion attacks. Our scheme provides security against chosen plain-text attacks under the k-multi-linear Decisional Diffie-Hellman assumptions. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

Keywords: Cipher-text-policy attribute-based encryption, hybrid encryption, user revocation, circuits, multi-linear map.

1. INTRODUCTION

Cloud computing is an on requested service in which shared data, information, software and other devices are provided according to the user at that time. Within this computing environments, the cloud servers can validate numerous data services, such as access control data, which has to be accessed by, authorize centralized users. For delegation computation, the server could be used to handle and calculate numerous data according to the user's needs. Presently the use of cloud computing is tremendous. So confidentiality and delegation problems are arising. More present public key attribute methods allow a party to encrypt data to specific user, but are unable to effectively handle more expressive types of encrypted access control. So there is a need to enhance a security problem of cloud computing. As applications move to cloud computing platforms for the use of security, a ciphertext-policy attribute-based encryption and user revocation mechanism are used to validate the confidentiality and the authenticity of delegation on cloud servers. The rise of cloud computing conveys a progressive development to the administration of the data assets. Inside these computing conditions, the cloud servers can offer different data administrations, for example, remote data stockpiling and redistributed designation calculation, and so forth. For data stockpiling, the servers store a lot of shared data, which could be gotten to be approved users. For assignment calculation, the servers could be utilized to deal with and compute various data as per the user's requests. As applications move to cloud computing stages, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are utilized to guarantee the data privacy and the obviousness of appointment on deceptive cloud servers. Taking therapeutic data sharing for instance (see Fig.1), with the expanding volumes of restorative pictures and medicinal records, the human services associations put a lot of data in the cloud for reducing data stockpiling expenses and supporting therapeutic participation. Since

the cloud server may not be acceptable, the record cryptographic capacity is a viable technique to keep private data from being stolen or altered. Meanwhile, they may need to impart data to the individual who fulfills a few prerequisites. The prerequisites, i.e, get to arrangement, could be {Medical Association Membership ∧ (Attending Doctor ∨ Chief Doctor) ∧ Orthopedics}. To make such data sharing be accessible, attribute-based encryption is appropriate. Therapeutic data sharing framework there are two reciprocal types of attribute based encryption. One is key-policy attribute-based encryption (KP-ABE), and the other is ciphertext-policy attribute based encryption (CPABE). In a KP-ABE framework, the choice of access approach is made by the key merchant rather than the enciphered, which restricts the practicability and ease of use for the framework in reasonable applications. Despite what might be expected, in a CP-ABE framework, each ciphertext is related with an access structure, and every private key is marked with an arrangement of graphic attributes. A user can unscramble a ciphertext if the key's attribute set fulfills the structure related with a ciphertext. Obviously, this framework is theoretically nearer to conventional access control strategies. Then again, in an ABE framework, the access arrangement for general circuits could be viewed as the most grounded type of the strategy articulation that circuits can express any program of settled running time. Appointment computing is another fundamental administration given by the cloud servers. In the above situation, the social insurance associations store data documents in the cloud by utilizing CP-ABE under certain access policy arrangements. The users, who need to get to the data records, decide not to deal with the unpredictable procedure of unscrambling locally because of constrained assets. Rather, they are well on the way to redistribute some portion of the unscrambling procedure to the cloud server. While the untrusted cloud servers who can make an interpretation of the first ciphertext into a straightforward one could take in nothing about the plaintext from the assignment. Crafted by assignment is promising yet unavoidably experiences two issues.

The cloud server may alter the data proprietor's unique ciphertext for malicious attacks, and afterward react a false changed ciphertext. The cloud server may cheat approved user for cost sparing. In spite of the fact that the servers couldn't react a right changed ciphertext to an unapproved user, he could cheat an approved one that he/she isn't qualified. Further, the organizations of the capacity and appointment benefits, the primary necessities of this research are exhibited as follows.

A. Confidentiality

In recognize capacity under specific selected plaintext attacks. With the capacity benefit given by the cloud server, the redistributed data ought not be released regardless of whether malware or hackers invade the server. Furthermore, the unapproved users without enough attributes to fulfill the entrance policy couldn't get to the plaintext of the data. Moreover, the unapproved access from the untrusted server who acquires an additional change key ought to be prevented.

B. Verifiability

During the delegation computing, a user could approve whether the cloud server reacts a right changed ciphertext to encourage him/her decode the ciphertext instantly and effectively. To be specific, the cloud server couldn't react a false changed ciphertext or cheat the approved user that he/she is unapproved. Consequently, in this paper, we will endeavor to refine the meaning of CP-ABE with verifiable delegation in the cloud to think about the data classification, the fine grained data get to control and the certainty of the delegation.

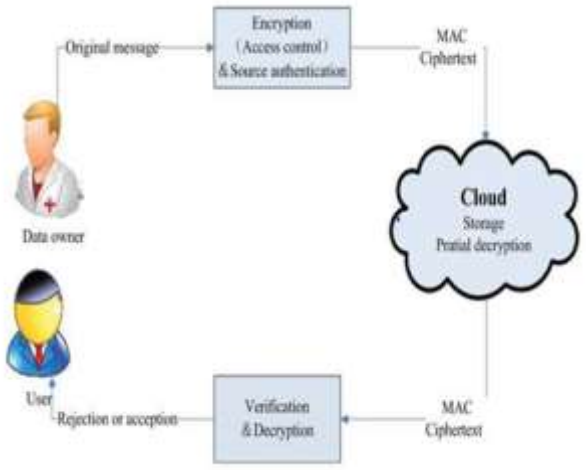


Fig. 1: Data Sharing System

Journal of Engineering Sciences
Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

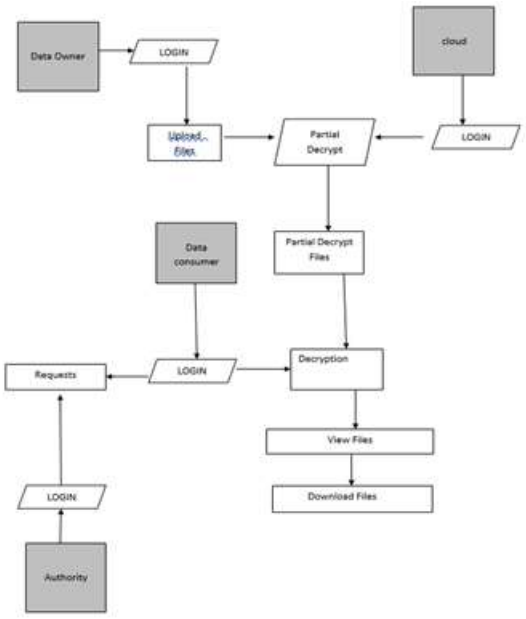


Fig. 2: Flow Chat

2. RELATED WORK

Attribute-based encryption (ABE) is a public-key based one-to-many encryption that enables users to scramble and decode data based on user attributes Different from personality based encryption conspire, an attribute-based encryption is a technique in which every user is recognized by an arrangement of attributes, and some capacity of those attributes is utilized to decide unscrambling capacity for each ciphertext [4].ABE comes in two quickness called key-policy ABE (KP-ABE) and ciphertext-policy ABE. In KP-ABE, attributes are utilized to depict the encoded data and approaches are incorporated with user's keys; while in CP-ABE, the attributes are utilized to depict a user's probate, and an encryptor decides a policy on who can decode the data [1]. Attribute-based encryption (ABE) is a public-key based one-to-numerous encryption that enables users to scramble and decode data based on user attributes [5]. In a decentralized attribute-based encryption (ABE) framework, any gathering can go about as a specialist by making a public key and issuing private keys to various users that reflects their attributes with no coordinated effort. Such an ABE plan can dispose of the weight of overwhelming correspondence and shared computation in the setup period of multi expert ABE plans, along these lines is viewed as more best [7]. With the developing prominence of cloud computing, associations and data owners begins to re-appropriate their critical data to the public cloud for reduce administration cost and straightforward entry. Encryption ensures user data confidentiality, it makes hard to perform secure plain text seek over the scrambled data [8]. In [10] the wide assortment of little, computationally powerless gadgets and the developing number of computationally serious undertakings makes it speaking to appoint computation to data focuses. In any case, redistributing computation is helpful just when the returned outcome can be believed, which makes verifiable computation (VC) an absolute necessity for such situations. In this work we expand the meaning of verifiable computation in two imperative ways: public delegation and public obviousness, which have essential applications in numerous available delegation situations.

3. PROPOSED SYSTEM

Attribute-based encryption the thought of attribute-based encryption (ABE). In consequent works, they concentrated on strategies over various experts and the issue of what articulations they could accomplish. As of not long ago, raised a development for acknowledging KPABE for general circuits. Before this strategy, the most grounded type of articulation is Boolean equations in ABE frameworks, which is as yet a long ways from having the capacity to express access control as any program or circuit. In reality, there still stay two issues. The first is their have no development for acknowledging CPABE for general circuits, which is adroitly nearer to conventional access control. The other is identified with the productivity, since the leaving circuit ABE conspire is a extent encryption one. Consequently, it is obviously still remains a significant open issue to plan an effective circuit CP-ABE scheme. Cross breed encryption the nonexclusive KEM/DEM development for half breed encryption which can encode messages of subjective length. Based on their quick work, a one-time MAC were joined with symmetric encryption to build up the KEM/DEM demonstrate for crossover encryption. Such enhanced model has the benefit of accomplishing higher security prerequisites. ABE with Verifiable Delegation. Since the presentation of ABE, there have been progresses in numerous ways. The use of redistributing computation is one of an imperative heading. The first ABE with redistributed unscrambling plan to reduce the computation cost amid decoding. The meaning of ABE with verifiable

re-appropriated decoding. They look to ensure the accuracy of the first cipher text by utilizing a dedication. Be that as it may, since the data proprietor produces a responsibility with no mystery esteem about his character, the un believed server would then be able to manufacture a dedication for a message he picks. Consequently the cipher text identifying with the message is in danger of being altered. Besides, simply alter the duties for the cipher text identifying with the message isn't sufficient.

S. No	Attribute	Owner	Access Control [N]	Access Permission Count [N]
1	Name	P	6	80
2	Age	Q	8	115
3	DOB	R	12	205
4	Salary	S	14	240
5	Attendance	T	19	355

The cloud server can misdirect the user with appropriate authorizations by reacting the terminator ⊥ to cheat that he/she isn't permitted to access to the data.

ALGORITHM:

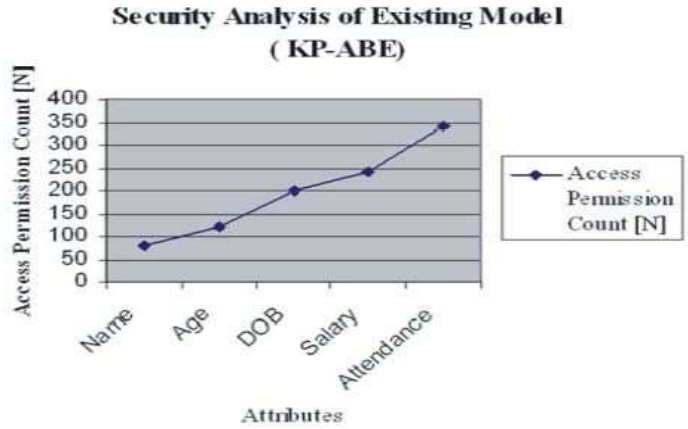
Cipher-text-Policy Attribute Based Encryption

A cipher-text policy attribute-based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, Key Gen and Decrypt.

i. Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

ii. Encrypt (PK, M, A): The encryption algorithm takes as input: the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

iii. Key Generation (MK, S): The key generation algorithm takes as input: the master key MK and a set of attributes S that describe the key. It outputs: private key SK.



iv. Decrypt (PK, CT, SK): The decryption algorithm takes as input: the public parameters PK, a cipher-text CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the cipher-text and return a message M.

v. Delegate (SK, S): The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S Ł S. It output a secret key SK for the set of attributes S.

The experimental result for existing Key-Policy ABE Algorithm model is represents in Table 1.1. The table shows the selecting the number of Attributes, Access control [15] count and Access permission count. The table contains the various attributes, owner and access policy control and access permission count.

Table- 1.1 Security Analysis of Existing Model (KP-ABE)

The experimental result for the proposed Cipher Text-Policy Attribute-Based Encryption (CP-ABE) with User Revocation model is represents in Table 1.2. The table shows the selecting the number of Attributes, Access control count and Access permission count [15]. The

table contains the various attributes, owner, and access policy control and access permission count.

S. No	Attribute	Owner	Access Control [N]	Access Permission Count [N]
1	Name	P	10	180
2	Age	Q	15	270
3	DOB	R	18	310
4	Salary	S	26	430
5	Attendance	T	28	520

Table 1.2: Security Analysis of proposed CP-ABE

The experimental result for proposed cipher-text Policy based ABE Algorithm model represents in Figure 5. It shows the selecting the number of Attributes and Access permission count based on the access control policy count.

The comparison result of existing Key-Policy ABE Algorithm and Cipher-text Policy base ABE is representing it shows the selecting the number of Attributes and Access permission count based on the access control policy count.

4. CONCLUSION

The proposed plan is ended up being secured based on k-multilinear Decisional Diffie-Hellman suspicion. Then again, we execute our plan over the whole numbers. The expenses of the computation and correspondence utilization demonstrate that the plan access in the cloud computing. In this way, we could apply it to guarantee the data privacy, the fine-grained get to control and the verifiable delegation in cloud. Presently we will encode the specific document and transferring it onto the cloud. For further improvements we can transfer immense data containing documents (it might be video, sound or some more). Indeed, even we can go for further live video spilling records by utilizing some great advancement like hadoop and start. Indeed, even we can include the idea of re-encryption of scrambled document. Further we can include the idea of auto activating SMS with OTP.

REFERENCES

[1]M. Armbrust, A. Fo x, R. Griffith, A. D. Joseph, R. H. Kat z, A.Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M.Zaharia , ”Above the Clouds: A Berkeley View of Cloud Co mputing, “Un iversity 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 SecuritySymp., 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, Efficient, 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 co mputation 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,

[8]Springer-Verlag Berlin, Heidelberg, 2012.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 fro m Multilinear Maps,” in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin, Heidelberg, 2013.

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