IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-4 E-ISSN: 2347-2693

KDC Based KP-ABE for Data Encryption in Cloud

Reenu Lathwal[1] and Vinod Kumar Saroha[2*]

[1,2*] SES, B.P.S.M. University Khanpur Kalan Sonipat (Haryana), INDIA

www.ijcseonline.org

Received: April /02/2015 Revised: April/11/2015 Accepted: April/23/2015 Published: April/30/ 2015

***Abstract*—** There are lots of cipher-text policies to provide control access mechanism. Attribute-based encryption reconsiders the concept of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In this, the decryption of a ciphertext is possible if the set of attributes of the user key matches the attributes of the ciphertext. File distribution and sharing is the most commonly used services in the cloud computing. Attribute based encryption is the attractive way to manage and control file sharing in cloud with its special attribute computing properties. Attribute-based encryption (ABE) is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. The authors take a centralized approach where a key distribution center (KDC) distributes secret keys and attributes to all users. Cloud computing is a new concept of computing technique, by which computer resources are provided dynamically via internet. Decentralized scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme supports creation, modification, and reading the data stored in cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.

Keywords**—** Access Control, Cloud Computing, Data Privacy, Fine-Grained Access Control, Attribute-Based Encryption, Ciphertext Policy

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction . There are two main categories of cloud infrastructure: public cloud and private cloud. To take advantage of public clouds, data owners must upload their data to commercial cloud service providers which are usually considered to be semi trusted, that is, honest but curious. That means the cloud service providers will try to find out as much secret information in the users' outsourced data as possible, but they will honestly follow the protocol in general. Traditional access control techniques are based on the assumption that the server is in the trusted domain of the data owner, and therefore an omniscient reference monitor can be used to enforce access policies against authenticated users. However, in the cloud computing paradigm this assumption usually does not hold, and therefore these solutions are not applicable. There is a need for a decentralized, scalable, and flexible way to control access to cloud data without fully relying on the cloud service providers. Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In traditional public key encryption or identity-based encryption systems encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

Corresponding Author: *Vinod kumar saroha, vnd.saroha@gmail.com*

Ciphertext-Policy ABE

In ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext. Policies may be defined over attributes using conjunctions, disjunctions and (k, n)-threshold gates, i.e., k out of n attributes have to be present (there may also be non-monotone access policies with additional negations and meanwhile there are also

© 2015, IJCSE All Rights Reserved

constructions for policies defined as arbitrary circuits). For instance, let us assume that the universe of attributes is defined to be {A, B, C, D} and user 1 receives a key to attributes {A, B} and user 2 to attribute {D}. If a ciphertext is encrypted with respect to the policy (A∧C) ∨D, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.

CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice feature is that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows decrypting. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

Key-Policy ABE

KP-ABE is the dual to CP-ABE in the sense that an access policy is encoded into the users secret key, e.g., (A∧C)∨D, and a ciphertext is computed with respect to a set of attributes, e.g., {A,B}. In this example the user would not be able to decrypt the ciphertext but would for instance be able to decrypt a ciphertext with respect to {A, C}.

An important property which has to be achieved by both, CP- and KP-ABE is called collusion resistance. This basically means that it should not be possible for distinct users to "pool" their secret keys such that they could together decrypt a ciphertext that neither of them could decrypt on their own (which is achieved by independently randomizing users' secret keys).

II. RELATED WORK

The scheme uses a symmetric [1] key approach and does not support authentication. Symmetric key algorithm uses same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. The validity of the user who stores the data is also verified. The proposed scheme is resilient to replay attacks. In this scheme using Secure Hash algorithm for authentication purpose, SHA is the one of several cryptographic hash functions, most often used to verify that a file has been unaltered. The Paillier crypto system is a probabilistic asymmetric algorithm for public key cryptography. Paillier algorithm use for Creation of access policy, file accessing and file restoring process. This paper [2] has constructed a new KP-ABE scheme supporting any monotonic access structure with constant size ciphertext and proved that the proposed scheme is semantically secure in selective-set model based on the general Diffie-Hellman exponent assumption. The downside of the proposed KP-ABE scheme is that private keys have multiple size growths in the number of attributes in the access structure. One interesting open problem would be to construct a KP-ABE scheme with constant-size cipher texts that is secure under a more Standard assumption or which achieves a stronger full security notion. Another challenging problem is to construct a KP-ABE scheme with constant ciphertext size and constant private key size. This paper [3] presents an anonymous privilege control scheme Anony Control to address not only the data privacy problem in cloud storage, but also the user identity privacy issues in existing access control schemes. By using multiple authorities in cloud computing system, our proposed scheme achieves anonymous cloud data access and fine-grained privilege control. Our security proof and performance analysis shows that Anony Control is both secure and efficient for cloud computing environment. In the proposed [4] scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing data. Decentralized scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. This scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud and also address user revocation. If multiple authorities [5] are corrupted, they cannot collect the user's attributes by tracing his GID. Notably, our scheme only requires standard complexity assumptions (e.g., decisional bilinear Diffie-Hellman) and does not require any cooperation between the multiple authorities, in contrast to the previous comparable scheme that requires non-standard complexity assumptions (e.g., q-decisional Diffie-Hellman inversion) and interactions among multiple authorities. As cloud has become [6] alternative solution for storing huge amount of data and processing, the research on data sharing and security has assumed importance. Recently Liu et al. have provided a comprehensive solution for member and data dynamics in cloud computing environment where members belong to a group and group manager can have provision to revoke users. Users can dynamically add and get revoked from the group making it a dynamic group. A framework [7] of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. In this paper, author proposed [8] the secure data storage in clouds for a new decentralized access. The cloud

© 2015, IJCSE All Rights Reserved

verifies the authenticity of the series without knowing the user's identity in the proposed scheme. Our feature is that only valid users can able to decrypt the stored information. It prevents from the replay attack. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.

III. PROBLEM FORMULATION

There are some problem come under this technique:-

- The problem with KP-ABE scheme is the encryption cannot decide who can decrypt the encrypted data. So main problem in this to find user who decrypt the encrypted data.
- The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data.
- The application of this scheme is restricted in the real environment because it use the access of monotonic attributes to control user's access in the system.

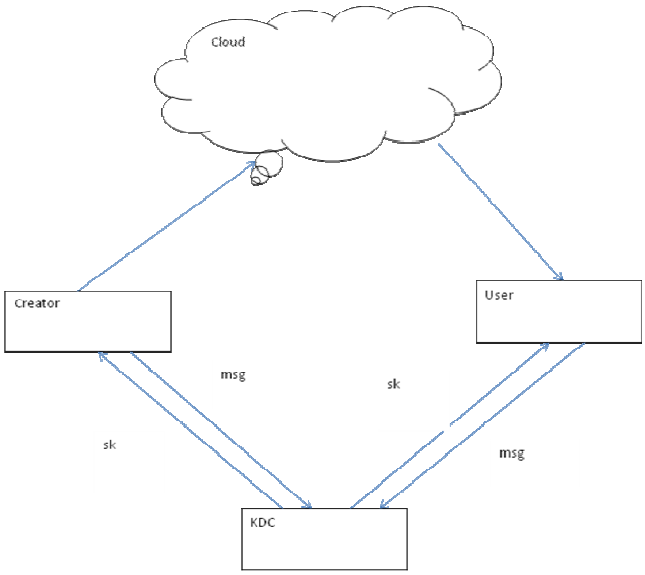
IV. PROPOSED WORK

In traditional public key encryption or identity-based encryption systems encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. In define attribute policies it has been observed that cipher text size is dependent on cipher attributes. If attributes are more than key size also increases.

Following will be our key objectives which will be achieved during our work:

- Key-Policy Attribute Based Encryption of data stored in cloud will allow only the authorized users and only valid users are able to access and modify the data stored in cloud.
- Here the key distribution center (KDC) is used to distribute the keys using Escrow-Free Key Issuing Protocol. It will help to multiple read and write on data stored in cloud environment.
- The architecture is decentralized, meaning that there should be several KDCs for key management.
- During authentication, the user personality will be protected.
- Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. The identity of the user is protected from the cloud during authentication.

A block diagram for this is shown in figure. Its key generation procedure is modified for our purpose of removing escrow. The proposed scheme is then built on this new CP-ABE variation by further integrating it into the proxy re-encryption protocol for the user revocation. To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group which is related to TPA permission generated code, since otherwise revocation cannot take effect after all.



Fine-grained access control: - It granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Access control relies on software checks to ensure that a user can access a piece of data only if he is authorized to do so.

Secret-sharing schemes (SSS): - It is used to divide a secret among a number of parties. The information given to a party is called the share for that party. In SSS, one can specify access tree structure where the interior nodes consist of AND and OR gates and the leaves consist of different parties.

KP-ABE: - KP-ABE can achieve fine-grained access control and more flexibility to control users than ABE scheme. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes in this secret key of the user is defined. KP-ABE defines four algorithms to achieve access control:-

Setup: - In this, we provide K as input and it generate output PK as a public key with MK.PK as a master key. MK is

© 2015, IJCSE All Rights Reserved

used to generate user secret keys and is known only to the authority.

Encryption: - It takes message M, public key PK and set of attributes as a input and it generate ciphertext E as output.
Key generation: - In this, access structure T and Master secret key (MK) used as a input and SK to decrypt a message if T matches as output.

Decryption: - It takes SK for access structure T and ciphertext E as input and give message M if and only if the attributes set satisfies the users access structure T as output.

Proposed scheme: - In this scheme there are many activities such as system initialization, user registration, user revocation, file generation, file deletion. In this paper our focus is to use cloudsim to implement the scheme and original dynamic broadcast encryption (ODBE).

Cloudsim: - It is JAVA based simulation tool. It is a simulation framework for modeling and simulating cloud computing environments. Cloudsim helps in simulating data centers, virtualized servers, energy-aware computational resources, network topologies, federated clouds, simulation elements and virtual machines etc.

Conclusion and future work

In this paper we studied the problem of secure and privacy preserving data sharing among the groups of users of cloud. As cloud has become solution for storing large amount of data and processing, the research on data sharing and security has assumed importance. In this paper, we use Cloudsim simulation tool which is specially designed for cloud simulations. The simulation results are encouraging. Simulating quality of service of cloud data center and cloud federation are the directions for future work. In future, I would like to hide the attributes and access policy of a user. In this, I would like to generate a key to make ciphertext more secure. Attribute based encryption method is also generated for cloud computing.

REFERENCES

[1]. M. Suriyapriya, A. Joicy," Attribute Based Encryption with Privacy Preserving In Clouds", International Journal on Recent and Innovation Trends in Computing and Communication, Volume 2 Issue 2, February 2014,

[2]. Changji Wang, Jianfa Luo," An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" Mathematical Problems in Engineering Volume 2013

[3]. Taeho Jung , Xiang-Yang Li , Zhiguo Wan," Privacy Preserving Cloud Data Access With Multi-Authorities" arXiv:1206.2657v6 [cs.CR] 11 Apr 2013

[4]. Geetanjali. M, Saravanan. N," Attribute Based Encryption with Privacy Protection in Clouds" International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014

[5]. Jinguang Han, Student Member, IEEE, Willy Susilo, Senior Member, IEEE, " Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption". IEEE Transactions on Parallel And Distributed Systems Vol.23 No.11, 2012

[6]. Moligi Sangeetha," Simulation of Secure Data Sharing Scheme for Dynamic Groups in Cloud" International Journal of Computer Engineering and Applications, Volume VII, Issue II, August 14

[7]. M. Vijayapriya, Dr. A. Malathi," On Demand Security for Personal Health Record in Cloud Computing Using Encryption and Decryption Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013

[8]. A.Vijayalakshmi, R.Arunapriya," Authentication of Data Storage Using Decentralized Access Control In Clouds" JGRCS, Volume 5, No. 9, September 2014

[9]. Geetanjali.M, Saravanan.N, " attribute based encryption with privacy protection in clouds" IJIRCCE, Vol.2, special issue 1, march 2014

[10]. Moligi Sangeetha, "simulation of secure data sharing scheme for dynamic groups in cloud" IJCEA, Vol.7, issue 2, august 2014

[11]. E. Kamalakannan, Arvind .K.S," Investigation on Improving the Security of Public Health Record System in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 8, October 2013

[12]. M. Suriyapriya, A. Joicy, "attribute based encryption with privacy preserving in clouds", IJRITCC, VOL.2, Issue 2, Feb. 2014.

[13]. A.Malathi, M.vijayapriya, "on demand security for personal health record in cloud computing using encryption and decryption cryptography", IJARCSSE, Vol. 3, Issue 9, sep.2013.

[14]. A.Vijayalakshmi, R.Arunapriya, "authentication of data storage using decentralized access control in clouds", JGRCS,Vol.5, No.9, sep. 2014.

[15]. Minu George, Dr. C.Suresh Gnanadhas, Saranya.K," A Survey on Attribute Based Encryption Scheme in Cloud Computing"IJARCCE, Vol.2, issue 11, nov.2013.

[16]. M. Suriyapriya, A. Joicy, "Attribute Based Encryption with Privacy Preserving In Clouds", IJRITCC, Vol.2, issue 2, feb.2014.

© 2015, IJCSE All Rights Reserved

[17]. Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang," A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013.

[18]. Vipul goyal, omkant pandey, "attribute-based encryption for fine-grained access control of encryption data".

© 2015, IJCSE All Rights Reserved