INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 2057-5688

SECURE INFORMATION TEAM SHARING AND CIRCULATION WITH CHARACTERISTICS AND TIME CONDITIONS IN PUBLIC CLOUD

E.NAGESWARARAO [1], V.SUDHAKAR [2], Y.SARASWATHI [3], M.PRATHYUSHA [4]

[1, 2, 3, 4]Assistant Professor, Department of CSE, *MALINENI LAKSHMAIAH WOMEN'S ENGINEERING COLLEGE*, Guntur - Prathipadu Rd, Pulladigunta, Andhra Pradesh , India.

ABSTRACT:

With the fast advancement of cloud administrations, immense volume of data is shared through cloud computing. Albeit cryptographic methods have been used to give data secrecy in cloud computing, current instruments can't authorize protection worries over ciphertext related with multiple owners, which makes co-owners unfit to suitably control whether data disseminators can really scatter their data. In this paper, we propose a safe data group sharing and restrictive dispersal conspire with multi-owner in cloud computing, in which data owner can impart private data to a group of clients by means of the cloud in a safe manner, and data disseminator can spread the data to another group of clients if the qualities fulfil the entrance approaches in the ciphertext. We further present a multiparty get to control instrument over the scattered ciphertext, in which the data co-owners can annex new access approaches to the ciphertext because of their protection inclinations. In addition, three arrangement collection methodologies, including full grant, owner need and lion's share license, are given to tackle the protection clashes issue brought about by various access strategies. The security investigation and test results show our plan is useful and effective for secure data offering to multi-owner in cloud computing.

Keywords: Cloud, ciphertext, security, data security, key generation..

1. INTRODUCTION:

Cloud computing reverence is gained from the benefits of rich storage supplies and instantaneous feedback. Computer network assets are distributed, and on-demand support is delivered over the Internet. A number of businesses, such as Google, Alibaba and Amazon, have made public cloud services available. Individual users and business users upload data to the

ISSN : 2057-5688

cloud service provider (CSP) with the aid of these service providers, which serves data accessibility purposes from anywhere at any time and data can also be exchanged with others. In order to strengthen users' privacy concerns, most cloud services maintain access control list (ACL) to achieve control of access. And so on, users can either choose to give access rights to certain approved persons, or can choose to open their data to anyone. The CSP stores the data in plaintext form, which raises concerns about security threats between users. When the data is released to the CSP, the owner of the data loses power. CSP implements an assigned protocol that makes it a semi trusted server, where it may use the user's data for profit without the user's permission, this data is of significant interest to other users who would use the data to know the user's behavioural habits. The powerful findings are motivated by these protection and privacy issues surrounding data confidentiality. To achieve safe data sharing in cloud computing, it is important to implement access control mechanisms. Techniques such as attribute based encryption (ABE), remote attestation and identity based broadcast encryption (IBBE) are currently being used to resolve the security concerns. ABE is one of the tools used in cloud computing to share the data and to protect the data. ABE attributes a system for access control of the encrypted data using the access policies. Another tool used for cloud computing is IBBE where, for considering their specific I d or email, the data can be exchanged between multiple receivers at a time. IBBE is easier to assign data to individual users because it provides low-cost key management and comparatively smaller policy sizes. The owner of the data can securely share data using these mechanisms, thereby encouraging more users to share their data via cloud. These encryption mechanisms do not assist in cloud computing with data distribution but they may prevent unauthorized. Organizations from accessing the data. And after the data is encrypted and disseminated, it is not possible to make any changes to the ciphertext that the data owner uploads. The proxy re-encoding scheme (PRE) is used to achieve safe data transmission in cloud computing by entrusting the CSP with a re-encoding key associated with the new receivers. Reencryption key cannot meet some of the criteria, as the day owner can allow data disseminator to disseminate similar data only. Therefore, this problem is discussed in

ISSN : 2057-5688

the definition called conditional PRE (CPRE). Where one can reencrypt unique ciphertext. The conventional CPRE embraces only basic keywords, which is why they cannot address the dynamic scenarios that have arisen in cloud computing. Attribute-based CPRE is designed to support descriptive conditions, rather than keywords, which would enforce a ciphertext access policy. In this way the data owner will configure the fine-grained distribution condition for the shared data. Cloud computing's popularity is born from the advantages of rich stockpiling assets and the time to come. This summarizes the computing platform properties and ultimately offers on-demand advantages over the Internet. Numerous esteemed companies, for example Amazon, Google, Alibaba, are currently offering transparent cloud administrations. Such administrations allow individual customers and undertaking customers to move data (e.g. images, records and reports) to cloud specialist organization (CSP), to access data anywhere, and to give data to others. Most cloud administrations maintain control by holding up to the control list (ACL) in order to ensure client security.

OBJECTIVE:

Cloud computing has become increasingly popular among users and businesses around the world. Although cryptographic techniques can provide data protection for users in public cloud, several issues also remain problematic, such as secure data group dissemination and fine-grained access control of time-sensitive data. In this paper, we propose an identity based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a re-encryption key to cloud server. The re-encryption conditions are associated with attributes and releasing time, which allows data owner to enforce fine-grained and timed-release access control over disseminated ciphertexts. The theoretical analysis and experimental results show our proposed scheme makes a

ISSN : 2057-5688

trade off between computational overhead and expressive dissemination conditions.

2. LITERATURE SURVEY:

1) A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing

AUTHORS: K. Liang, M. H. Au, J. K. Liu, and W. Susilo In this paper, for the first time, we define a general notion for proxy re-encryption (PRE), which we call deterministic finite automata-based functional PRE (DFA-based FPRE). Meanwhile, we propose the first and concrete DFA-based FPRE system, which adapts to our new notion. In our scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-ciphertext secure in the standard model.

2) Identity-Based Broadcast Encryption with Constant Size Cipher texts and Private Keys

AUTHORS: C. Delerablée, This paper describes the first identity-based broadcast encryption scheme (IBBE) with constant size ciphertexts and private keys. In our scheme, the public key is of size linear in the maximal size *m* of the set of receivers, which is smaller than the number of possible users (identities) in the system. Compared with a recent broadcast encryption system introduced by Boneh, Gentry and Waters (BGW), our system has comparable properties, but with a better efficiency: the public key is shorter than in BGW. Moreover, the total number of possible users in the system does not have to be fixed in the setup.

3) Practical Identity-based Private Sharing for Online Social Networks

AUTHORS: F. Beato, S. Meul, and B. Preneel Online Social Networks (OSNs) constitute vital communication and information sharing channels. Unfortunately, existing coarse-grained privacy preferences insufficiently protect the shared information.

ISSN : 2057-5688

Although cryptographic techniques provide interesting mechanisms to protect privacy, several issues remain problematic, such as, OSN provider acceptance, user adoption, key management and usability. To mitigate these problems, we propose a practical solution that uses Identity-Based Encryption to simplify key management and enforce data confidentiality. Moreover, we devise an Identity-Based outsider anonymous private sharing scheme to disseminate information among multiple users. Furthermore, we demonstrate the viability and tolerable overhead of our solution via an open-source prototype.

4) Cipher text-policy Attribute based Encryption

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters, In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

5) Fuzzy Keyword Search over Encrypted Data in Cloud Computing

AUTHORS: Z. Wan, J. Liu, and R. Deng

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based

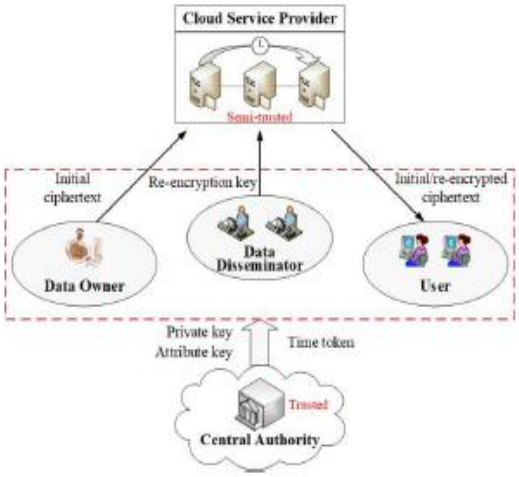
ISSN : 2057-5688

encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bettencourt and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

In this paper, we propose a secure data group sharing and dissemination scheme with attribute and time conditions in public cloud. The main contributions of our scheme are as follows, we employ IBBE technique to achieve secure data group sharing in public cloud, which allows data owner to outsource encrypted data to semi-trusted cloud and share it with a group of receivers at one time. It is more convenient that email and username could be used as public keys for users. We design an access policy embedding releasing time and take the advantages of attribute-based CPRE, to achieve fine-grained and timed-release data group dissemination. The CSP can re-encrypt initial ciphertexts for data disseminator after the designate time if his attributes associated with the re-encryption key satisfy the access policy in the ciphertexts. We analyze the security of our proposed scheme, and conduct a detailed theoretical and experimental analysis. The results show that our scheme makes a tradeoff between computational overhead and expressive dissemination conditions, and performs significantly better in data group sharing and dissemination in public cloud.

3. PROPOSED SYSTEM:

ISSN : 2057-5688



In order to secure data group sharing, identity-based broadcast encryption (IBBE) is employed in public cloud. The data owners could broadcast their encrypted data to a group of receivers at one time and the public key of the user can be regarded as email, unique id and username. Hence, by using an identity, data owner can share data with other group users in a convenient and secure manner. Attribute-based encryption (ABE) is one of new cryptographic mechanisms used in cloud to reach flexible and fine-grained secure data group sharing. Especially, cipher text-policy ABE (CP-ABE) allows data owners to encrypt data with an access policy such that only users whose attributes satisfy the access policy can decrypt the data. To propose a practical TRE (Timed-Release Encryption) system, using a trusted time agent rather than data owner to uniformly release the access privilege at a specific time. A predicate encryption based secure data storage scheme called TR-CPBRE, by integrating TRE into data access control, in which the evaluator decrypts the cipher texts that satisfy the predicate only after a specified time period.

4. IMPLEMENTATION WITH RESULTS EXPLANATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Dissemination Conditions:

Let T denote an access tree, a logical representation of an access policy. Each non-leaf node x represents a threshold gate, described by its children and a threshold value. Let numx denote the number of children of a node x, and kx represent its

ISSN : 2057-5688

threshold value. For each leaf node y, we have ky = 1. Let attry denote an attribute associated with leaf node y in the tree and parent(z) represent a parent node of the node z in the tree. Each child node of the node x in the tree is labeled from 1 to numx, and index(x) returns such label associated with the node x. These index values are uniquely assigned to nodes in the access tree in an arbitrary manner. Let Tx be a subtree of T rooted at the node x. If a set of attributes r satisfies access tree Tx, we denote it as Tx(r) = 1. We compute Tx(r) recursively as follows. For a non-leaf node x, it evaluates Tz(r) for all children z of node x. For non-leaf node x, Tx(r) returns 1 if and only if at least kx children return 1. For the leaf node y, it retu rns 1 if and only if attry ∈ r.

Identity-Based Broadcast Encryption:

The IBBE scheme allows data owner to encrypt a message only once for many receivers via the broadcast channel. The data owner does not hold any private information and the encryption are performed with a set of identities of the receivers, which can be seen as an extension of the IBE. The definition of IBBE is given below.

1) Setup (1X , N): On input a security parameter X and the maximal size N of a set of receivers for an encryption, this algorithm outputs a pair of public key PK and master secret key MK.

2) KeyGen (PK, MK, ID): On input an identity ID, the public key PK and the master secret key MK, this key generation algorithm outputs a secret key SK for user ID.

3) Enc (PK, U, M): On input a set U of identities, the public key PK and a message M, the algorithm outputs a ciphertext CT for U.

4) Dec (PK, CT, SK, ID): On input the public key PK, the ciphertext CT and the secret key SK, the algorithm outputs the message M if ID ∈ U.

Ciphertext-Policy Attribute-Based Encryption:

The CP-ABE is a cryptography prototype for one-to-many secure communication, in which the data owner shares data to the intended users by designating an access policy and encrypting the data under the access policy. In CPABE based approach, the access policy is expressed as a tree over a set of attributes and logic gates. Each user obtains the secret key from the authority based on the attributes. It consists of

ISSN : 2057-5688

following algorithms [36]. 1) Setup(1): The setup algorithm takes as input the security parameter and outputs a public key PK and a master secret key MK. 2) KeyGen(PK, MK, S): The key generation algorithm takes as input the public key PK, the master secret key MK, a set S of attributes, and outputs an attribute key SK. 3) Enc(PK, M, T): The encryption algorithm takes as input the public key PK, a message M and an access policy T, and outputs a ciphertext CT.4) Dec(PK, SK, CT): The decryption algorithm takes as input the public key PK, an attribute key SK, a ciphertext CT with an access policy T. I S ∈ T, it outputs the message M.

Timed-Release Encryption:

The TRE allows data owner to encrypt message for the purpose that intended users can decrypt it after a designated time. It is a two-factor encryption scheme combining public key encryption (PKE) and timedependent encryption. In order to recover message, a trusted agent is required to expose time token, which is kept confidential by the trusted agent until at an appointed time, thus even the intended user cannot get the plaintext of message before the designated releasing time.

1) Encryption. When encrypting message, the ciphertext is generated with the public key of the intended user and the designated releasing time t.

2) Decryption. At each time point t, the trusted agent releases a time token TKt. The ciphertext holds the feature that only with corresponding user's secret key and time token TKt, can a user correctly get the plaintext; otherwise, the user cannot conduct the decryption successfully.

5. CONCLUSION:

In this paper, we propose a secure data group sharing and dissemination scheme in public cloud based on attribute- based and timed-release conditional identity based broadcast PRE. Our scheme allows users to share data with a group of receivers by using identity such as email and username at one time, which would guarantee data sharing security and convenience in public cloud. Besides, with the usage of fine-grained and timed-release CPRE, our scheme allows data owners to custom access policies and time trapdoors in the cipher text which could limit the dissemination conditions when outsourcing their data. The CSP will re-encrypt the cipher text successfully only when the attributes of data disseminator

ISSN : 2057-5688

associated with the re-encryption key satisfy access policy in the initial cipher text and the time trapdoors in the initial cipher text are exposed. We conduct our experiments with pairing based cryptography library. The theoretical analysis and experiment results have shown the security and efficiency of our scheme.

REFERENCES:

[1] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[2] C. Delerablée, "Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys," Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215, 2007.

[3] F. Beato, S. Meul, and B. Preneel, "Practical Identity-based Private Sharing for Online Social Networks," Computer Communications, vol. 73, pp. 243-250, 2016.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy Attributebased Encryption," Proc. the 28th IEEE Symposium on Security and Privacy (S&P 2007), pp. 321-334, 2007.

[5] Z. Wan, J. Liu, and R. Deng, "HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012.

[6] H. Hu, G. Ahn, and J. Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp. 1614-1627, 2013.

[7] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc. Advances in Cryptology- EUROCRYPT 1998 (EUROCRYPT '98), pp.127-144, 1998.

[8] D. Tran, H. Nguyen, W. Zha, and W. Ng, "Towards Security in Sharing Data on Cloud based Social Networks," Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011), pp. 1-5, 2011.

[9] J. Weng, R. Deng, X. Ding, C. Chu, and J. Lai, "Conditional Proxy Re-Encryption Secure Against Chosen-ciphertext Attack," Proc. the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (CCS 2009), pp. 322-332, 2009.

ISSN : 2057-5688

[10] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional Identity based Broadcast Proxy Re-encryption and its Application to Cloud Email," IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79, 2016.

[11] Y. Yang, H. Lu, J. Weng, Y. Zhang, and K. Sakurai, "Fine-grained Conditional Proxy Re-encryption and Application," Proc. the 8th International Conference on Provable Security (ProvSec 2014), pp. 206-222, 2014.

[12] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud," Proc. 2015 IEEE Global Communications Conference (GLOBECOM 2015), pp. 1-6, 2015.

[13] R. Rivest, A. Shamir, and D. Wagner, "Time Lock Puzzles and Timed-release Crypto," Massachusetts Institute of Technology, MA,
USA, 1996.