INTERNATIONAL JOURNAL ★ ENGINEERING RESEARCH
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 22nd Sept2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-8

Title: **ATTRIBUTE BASED REVOCABLE DATA ACCESS CONTROL FOR MULTI AUTHORITY CLOUD STORAGE WITH THE USAGE OF CP-ABE**

Volume 06, Issue 08, Pages: 320– 326.

Paper Authors

JETTI MANOHAR,KURREMULA JYOTHI

Vidya Jyothi Institute Of Technology, Aziz nagar, Hyderabad, Telangana, India

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ATTRIBUTE BASED REVOCABLE DATA ACCESS CONTROL FOR MULTI AUTHORITY CLOUD STORAGE WITH THE USAGE OF CP-ABE

[1]JETTI MANOHAR, [2]KURREMULA JYOTHI

[1]M.Tech Scholar, Dept of CSE, Vidya Jyothi Institute Of Technology, Aziz nagar, Hyderabad, Telangana, India

[2] Assistant Professor, Dept of CSE, Vidya Jyothi Institute Of Technology, Aziz nagar, Hyderabad, Telangana, India.

[1]manohar.jetti@gmail.com [2]jyothi.kurremula@gmail.com

ABSTRACT— Cloud computing is the essential computing model which allows the customers to save their information in to cloud. Attribute-Based control scheme establish permission to the media in the cloud where it makes use of cipher-text content policy Attribute-Based Encryption (CP-ABE) approach to create access control. These approaches inside access to coverage the attributes are used to generate a public key with the purpose to encrypt the records and a secret key with the purpose to decrypt the statistics. This paper gives a unique Multi-message Cipher text Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an acquire access control scheme for sharing scalable media based completely on data users attributes (e.g., age, nationality, or gender)as different to an express listing of the consumers names. The scheme is efficient and flexible due to the information MCP-ABE allow a content provider to specify an purchase access policy and encrypt a couple of messages inside one Cipher text such that most effective the customers whose attributes satisfy the get right of entry to policy can decrypt the Cipher text. Moreover, the paper shows the way to assist useful resource-restrained mobile devices through offloading computational in intensity operations to cloud servers even as without compromising account privacy.

Keywords: Access control, data storage, Multi-Authority

1. INTRODUCTION

Cloud computing is a reasonably evolved invention to store information from multiple consumer. Cloud computing is an environment that permits customers to remotely store their information. Remote backup device is the advanced concept which reduces the cost for implementing greater reminiscence in an agency. Because the cloud server can not be absolutely trusted with the aid of records proprietors, they could now not rely upon servers to do observe control. Cipher text-Policy Attribute-based Encryption(CP-ABE) is taken into consideration as one of the most appropriate technology for data study control in cloud loading structures, as it offers the records owner more apparent manage on study procedure. The CP-ABE scheme, there may be an evidence this is conscientious for factors management and key allocation .The proof can be the test office in a academia, the human useful resource branch in a organization, and many others. The statistics proprietor defines the study regulations and encrypts information in step with the guidelines. Each consumer may be introduced a self belief key redirecting its factors. A consumer can decrypt the information simplest when its elements satisfy the examiner policies. There are types of CP-ABE structures: unmarried-authority CP-ABE wherein all elements are managed by way of a unmarried- authority, and multi-authority CP-ABE in which factors are from one-of-a-kind domain names and controlled by using distinct evidences. Multi-authority CP-ABE is more appropriate for data examine manage of cloud loading systems, as customers may additionally keep study introduced by using multiple evidences and records proprietors can also proportion the facts the usage of examine guidelines described over study from one of a kind evidences. Now a days cloud computing is a rationally advanced generation to shop statistics from multiple client. Cloud computing is an environment that enables users to remotely save their facts. Remote backup system is the superior concept which reduces the cost for implementing extra reminiscence in an business enterprise. It enables organizations and government companies lessen their economic overhead of information control. They can archive their data backups remotely to third birthday party cloud garage providers rather than keep records facilities on their personal. An individual or an company may not require shopping the wished storage gadgets. Instead they can keep their records backups to the cloud and archive their facts to keep away from any statistics loss in case of hardware / software disasters. Even cloud storage is extra bendy, how the safety and privacy are to be had for the outsourced facts will become a extreme problem. There are three targets to be primary issue Confidentiality – preserving authorized restrictions on information get entry to and disclosure. The main danger done while storing the facts with the cloud. Integrity – guarding towards incorrect records amendment or destruction. Availability – making sure timely and dependable get admission to to and use of statistics. The Cloud Storage offers services for information proprietors to host their statistics into the cloud. A tremendous mission to records get entry to control scheme turned into records website hosting and information get right of entry to offerings. Because facts owners does now not fully agree with the cloud servers additionally they can now not depend upon servers to do get admission to manipulate The data access manage becomes a hard difficulty in cloud storage structures due to data outsourcing and untrusted cloud servers. Therefore Cloud garage is a model of records storage where the virtual information is stored in logical pool.

2. RELATED WORK

Attribute based accurate access control techniques allow flexible find access to strategy for the customers. However, they treated media content material as a single massive item, ignoring the structure of the content material. Hence, these schemes aren't suitable for obtain entry to manage to scalable multimedia content. Media Structure Oriented Access Control The SSS (Secure Scalable Streaming) encryption technique for scalable video is a modern encryption approach. As SSS encryption may additionally result in decryption rotate ups due to package deal loss , it must to be included with error correction strategies in exercise in order to overcome this problem. One of the most appropriate technologies for information access in cloud storage systems is Cipher text-Policy Attribute-based Encryption (CP-ABE). This scheme presents the records owner greater direct manipulate on get right of entry to rules. The Authority in CP-ABE scheme is chargeable for characteristic management and key distribution. The authority may be the college registration office, the human support department in a employer, and many others. The data proprietor in CP-ABE scheme defines the get right of entry to guidelines and encrypts information in keeping with the rules. CP-ABE TYPES: In CP-ABE scheme every user may be issued a mystery key reflecting its attributes. A user can decrypt the information simplest when its attributes fulfill the access guidelines.Applying the multi-authority schemes without delay to multi-authority cloud storage device is tough thanks to the characteristic revocation disadvantage. In multi-authority cloud storage systems, customers attributes is modified dynamically. A consumer may want to also be entitled some new attributes or revoked a few contemporary attributes. The permission of facts get admission to to be changed therefore. Existing characteristic revocation techniques either take delivery of a sincere server or lack of efficiency, they're no longer suitable for coping with the characteristic revocation disadvantage in information access manage in multi-authority cloud garage systems. Cipher text Policy-Attribute-Based Encryption, a gadget for realizing complicated get entry to manipulate on encrypted information will be predisposed to decision Cipher text Policy Attribute-Based encoding. By exploitation the strategies encrypted facts may be saved personal even though the storage server is entrusted, the techniques are secure against collusion assaults. Ciphertext-Policy Attribute-Based Encryption partner communicatory, Efficient and demonstrably Secure Realization present a technique for understanding Cipher text-Policy ABE systems from a widespread set of get admission to structures within the ordinary model beneath concrete and non-interactive assumptions. In any access manage scheme, there's an get admission to policy which defines the get entry to situations under which a subject can get entry to an item. An get entry to tree is a graph illustration of the get admission to coverage. Such a tree includes non leaf nodes and leaf nodes. Each leaf node is related to a person attribute (e.g., age, gender, career), even as every non-leaf node has toddler nodes which may be leaf nodes, other non-leaf nodes or both. The root, a unique non-leaf node, has no determine node.

3. FRAME WORK

Attribute Authority (AA), a depended on trusted party, set up the mechanism parameters of characteristic-based fully encryption machine (which includes device-huge public key and master key), verifies each person's attributes (e.g., group membership, role, security clearance or authorization records) and issues personal secret key corresponding to the set of attributes of the user. In practice, there may be multiple AAs in a machine. For example, a college or company may run an AA, and a person might also act as an AA for his/her extended circle of relatives participants. To preserve the presentation simple, we anticipate a unmarried AA in the relaxation of the paper. User may be a statistics owner, or a data patron, or each. A information proprietor produces (protected or unprotected) media content (textual content, voice, video, and many others.), and uploads the media content material to cloud servers. To put in force get entry to manipulate to his information, the information owner assigns assigns get entry to privileges to records clients whom the facts owner can also or might not know. A data client downloads media con-tent of interest from cloud servers, and obtains the content based on her attributes and the find admission to policy of the records owner. To this case, the data consumer should acquire from AA a personal secret key sure to her set of attributes. In this information owner-customer version, the backend servers -wide the fundamental platform for storage, networking, and many others; the foreground servers provide the interface for media time, transmission, and computational assistance to customers; while AA issues personal master keys so that find admission.

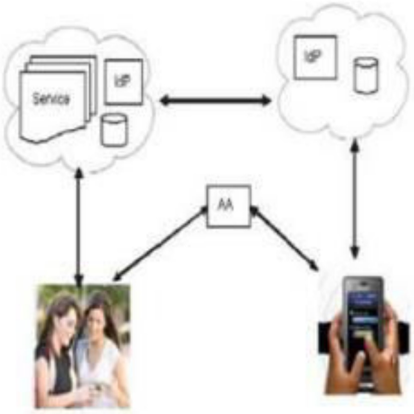

Figure1:System Architecture

In this paper we present an access control scheme for scalable media. The scheme has numerous benefits which make it specially suitable for content transport. For example, it's miles extremely scalable by way of permitting a statistics proprietor to provide statistics get right of entry to privileges primarily based on the facts purchasers attributes (e.g., age, nationality, gender) rather than an explicit list of user names; and it ensures information privacy and exclusiveness of get admission to of scalable media by means of using characteristic-based totally encryption. For this purpose, we introduce a singular Multi-message Cipher text Policy Attribute Based Encryption (MCP-ABE) technique. MCP-ABE encrypts a couple of messages within one cipher text with a purpose to implement bendy attribute-primarily based get entry to control on scalable media. Specifically, the scheme constructs a key graph which fits users' get admission to privileges, encrypts media units with the corresponding keys, after which encrypts the key graph with MCPABE; simplest the ones facts consumers with the specified user attributes can decrypt the encryption of the important thing (sub) graph and then decrypt the encrypted media gadgets. To cater for resource-limited cell gadgets, the scheme offloads computational in depth operations to cloud servers even as without compromising consumer information privateness. Components in an attribute - based access control scheme consists of topics each accurate by means of a fixed of attributes, objects and access rules. For example, a consumer's age, popularity, function are the difficulty attributes, at the same time as circulation files or presentation files are items. An find right of entry to policy defines the minimum characteristic set which a subject need to have so that you can get admission to the item. Therefore, the challenge in characteristic- primarily based access manipulate is the way to provide bendy and fine grained get right of entry to control at low value. An approach to access control in content material sharing services is to empower users to put into effect get admission to controls on their records at once, in preference to through a primary administrator. However, this calls for flexible and scalable cryptographic key management to assist complicated get entry to manipulate rules. A native get right of entry to manipulate solution is to assign one key for each consumer attribute, distribute the proper keys to customers who've the corresponding attributes, and encrypt the media with the attribute keys time and again.

4. EXPERIMENTAL RESULTS

To demonstrate the multi-level access control to manage, we built a presentation with one textual content record and generated the encrypted presentation and its permitting block with the method. In this section, help fine-grained find admission to manage rules and dynamic organization membership6 through the usage of CP-ABE scheme. In addition, is able to revoke a consumer with out issuing new keys to other users or re-encrypting present cipher-texts by the usage of a proxy. KP-ABE (Key Policy Attribute primarily based Encryption) to put in force get admission to regulations based totally on statistics attributes. Their scheme permits records owners to delegate maximum of the computation responsibilities worried in quality-grained information find admission to manage to untrusted cloud servers without disclosing the underlying statistics contents with the aid of combining strategies of characteristic-based totally encryption, proxy re-encryption, and lazy re-encryption an data management architecture the usage of CP-ABE and optimized safety. In this Module, each person's private secret key is related to a set of attributes while each cipher text is related to an get admission to policy. A person efficaciously decrypts a ciphertext most effective if her set of attributes satisfies the access coverage specific inside the ciphertext. We in short describe the CP-ABE. We will enlarge this CP-ABE scheme to MCPABE scheme and use the latter in our get admission to manage scheme. When a information owner bradcasts the encrypted content material, he has to broadcast the enabling block which is the communication overhead.

5. CONCLUSION

CP-ABE primarily based access control allows a information owner to enforce get admission to manipulate based on attributes of records consumers with out explicitly naming the specific information clients. However, CP-ABE supports only one privilege stage and hence isn't suitable for access manage to scalable media. In this paper we extended CP-ABE to a singular MCP-ABE and proposed a scheme to assist multi-privilege get entry to manipulate to scalable media. As cloud computing is more and more being followed and cell gadgets are becoming pervasive, the prevailing get entry to manage scheme permits a cell user to offload computational in depth MCP-ABE operations to cloud servers at the same time as without compromising consumer's safety. The experimental outcomes indicated that the proposed get right of entry to manipulate scheme is green for securely and flexibly coping with media content in large, loosely-coupled, dispensed structures. With the assistance of the cloud server, the decryption opera-tion is expanded extensively at the purchaser side. However, the decryption may be nevertheless sluggish for low-end devices because a modular exponentiation operation is needed.

6. REFRENCES

[1] E. Messmer, "Are Security Issues Delaying Adoption of Cloud Computing?" Network World, 2009-04-27.
[2] E. Messmer, "Security of Virtualization, Cloud Computing Divides IT and Security Pros", Networkworld.com, 2010-02-22.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy Attribute-based Encryption," IEEE Symposium on Security and Privacy, pp. 321-334, 2007.
[4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS Publication 180-1, 1995.
[5] P. Mell, and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, Sept. 2011.

[6] M.D. Soete, “Attribute Certificate,” Encyclopedia of Cryptography and Security, by Henk C. A. Van Tilborg, Sushil Jajodia (Eds), ISBN 978-1-4419-5907-2, pp.51, Springer. 2nd ed., Sept. 2011.

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage,” Network and Distributed System Security Symposium, 2005.

[8] X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu, “Toward a Usage-Based Security Framework for Collaborative Computing Systems”, ACM Trans. on Information and System Security, 11(1):1-36, 2008.

[9] S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation,” ACM 1 Symposium on Information, Computer and Communications Security, March 2011. 2

[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” IEEE 3 International Conf. on Computer Communications, pp. 1-9, 2010.