Attribute Based Access Control for Cloud Data Storage

Ninad Harke[1], Vishal Sherkar[2], Ajay Hadal[3], Nitin Dhawas[3]

[1,2,3]Student, Dept. IT Engineering, PCET's NMIET Pune, Maharashtra, India
[4] Professor, Dept. IT Engineering, PCET's NMIET Pune, Maharashtra, India

---***---

Abstract - *Fine grained access management could be a demand for knowledge stored in untrusted servers like clouds. Due to the massive volume of data, redistributed key management schemes square measure most popular over centralized ones. Usually coding and cryptography square measure quite expensive and not sensible once user's access knowledge from resource constrained devices. We tend to propose a redistributed attribute primarily based encryption (ABE) method with quick coding, outsourced cryptography and user revocation. Our scheme is incredibly specific to the context of mobile cloud because the storage of encrypted knowledge and therefore the partial decryption of cipher text square measure keen about the cloud and users with mobile devices will transfer knowledge to the cloud or access knowledge from it by acquisition little value for coding and cryptography respectively. The most plans is to divide the coding into 2 phases, offline pre-processing part that is completed once the device is otherwise not in use and an internet part once the info is truly encrypted with the policy. This makes coding quicker and a lot of efficient than existing decentralized ABE schemes. We also introduce user revocation during this theme while not acquisition too much additional value within the on-line part. Comparison with other ABE themes shows that our scheme considerably reduces computation times for each knowledge house owners and knowledge users and extremely suitable to be used in mobile devices.*

Key Words**: Attribute-based Encryption, User Revocation, Cloud Computing, Decentralized Key Management, Mobile Devices**

1. INTRODUCTION

Consider the common situation wherever information homeowners wish to transfer their information for semi-permanent storage to untrusted servers like the cloud [1]. The info might be initio reside in resource forced devices like mobile phones, wireless sensors or smartcards. The aim is to store the info over an extended time and permit multiple users to access the info. This information is sensitive and also the hospital might want solely the doctor attending a patient or a research worker concerned within the drug discovery to possess access to the info [4]. Secret writing schemes like attribute based secret writing (ABE) offer nice flexibility in terms of access management on encrypted information and square measure ideal for this situation [2],[3]. In observe, suburbanized or multi-authority ABE schemes square measure terribly helpful as they are doing not would like any central authority for generation and distribution of decoding keys associated with totally different attributes. For instance, the doctor UN agency needs to access a patient's health record for designation is also provided the relevant key by the hospital however a medical research worker is also given access to constant information by a medical analysis organization. We tend to propose a suburbanized attribute based mostly secret writing (ABE) theme with quick secret writing, outsourced decoding and user revocation [7].

Our theme is incredibly specific to the context of mobile cloud because the storage of encrypted information and also the partial decoding of cipher texts square measure passionate about the cloud and users with mobile devices will transfer information to the cloud or access information from it by acquisition little or no value for secret writing and de- 2 coding severally. As an answer to the pricey secret writing downside, we tend to divide the secret writing part into associate offline part and an internet part, such that, most of the pricey operations square measure performed offline once the user doesn't at once expect the secret writing to be completed, the device is charging or otherwise not in use the web part has very little computations in order that users will get on with their work while not the devices performance being affected in any respect [5]. Information user's square measure eased from activity pricey decoding operations by outsourcing such operations to a proxy server.

The proxy server, employing a reworked decoding key, partly decrypts the cipher text. However, the partial decoding method doesn't reveal any info to the malicious proxy server. Then, the info user has to perform solely a number of straightforward operations to derive the ultimate plaintext from the partly decrypted cipher text. Similarly, revocation keys are generated offline, with a number of computations within the on-line part for key transformation before they're given to the proxy server [1], [2].

2. Existing Methodology

2.1 Improving Privacy and Security in Multi-Authority Attribute- Based Encryption

Attribute based encryption (ABE) determines coding ability supported a user's attributes in a very multi-authority ABE scheme, multiple attribute authorities monitor totally different sets of attributes and issue corresponding decryption keys to users, and encryptions will require that a user acquire keys for applicable attributes from every authority before decrypting a message [1].

2.2 Identity Based and Attribute Based Cryptography: A Survey

Changing scenario of cryptography has led to a modification in paradigm of from certificate primarily based public keys and key rings to user- dependent keys that are based on identities of users or their attributes. This is often termed as identity based mostly cryptography or attribute based cryptography [2].

2.3 A Survey of Attribute-based Access Control with User Revocation in Cloud Data Storage.

Cipher text-policy attribute-based encryption may be a promising cryptologic resolution in cloud environment, which might be concerned for access management by the information owner to dene access policy [3]. Sadly, an outsourced architecture applied with the attribute-based encryption introduces several challenges during which one among the challenges is revocation [8]. The problem may be a threat to information security within the information owner.

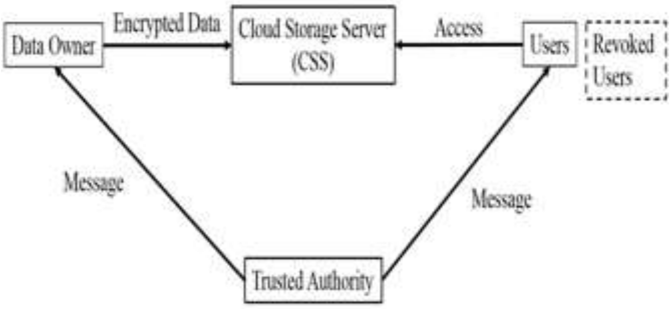

Fig. 1 The cloud storage architecture of attribute-based access control

2.4 Attribute-based data access control in mobile cloud computing: Taxonomy and open issues

ABE strategies and categorizes them into 3 main categories, like centralized, decentralized, and hierarchic, supported their architectures. We tend to conjointly analysed the various ABE techniques to determine the benefits and drawbacks, the importance and needs, and identifies the analysis gaps [4].

3. Scope

Our system can be used on daily basis instead of encrypting each part of a log with the keys of all recipients; it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.

4. Motivation

Access control is a requirement for data stored in untrusted servers like clouds. Often encryption and decryption are quite expensive and not practical when users access data from resource. Above mention problem exist in cloud computing so idea of Decentralized Attribute Based Access Control for cloud came in existence.

5. Disadvantages of Existing System

1. Single trusted party who store data and monitors all attributes.
2. We initial review some important Identity based encryption, signature and encryption schemes.
3. The problem may be a threat to information security within the information owner.
4. Taxonomy of attribute-based approaches supported important parameters, like access management mode, design, revocation mode, revocation technique, revocation issue, and revocation controller.

6. Proposed System

We propose a decentralized attribute primarily based encryption (ABE) theme with quick secret writing, outsourced cryptography and user revocation. Our theme is incredibly specific to the context of mobile cloud because the storage of encrypted information and also the partial decryption of cipher texts square measure smitten by the cloud and users with mobile devices will transfer information to the cloud or access information from it by acquisition little or no value for secret writing and cryptography respectively the most plan is to divide the secret writing into 2 phases, offline pre-processing section that is finished once the device is otherwise not in use and an internet section once the information is really encrypted with the policy. This makes secret writing quicker and a lot of efficient than existing decentralized ABE schemes. For cryptography outsourcing, information users got to generate a remodeled version of the cryptography key permitting associate degree untrusted proxy server to partly decrypt the cipher text while not gaining any info regarding the plaintext.

Information users will then absolutely rewrite the partly decrypted cipher text while not performing arts any pricey pairing operations. We also introduce user revocation during this theme while not acquisition too much extra value within the on-line section. Comparison with other ABE themes shows that our scheme considerably reduces computation times for each information homeowners and information users and extremely suitable to be used in mobile devices.

7. Advantages of Proposed system

1. Single trusted party who store data and monitors all attributes and issues all decryption keys.
2. Attribute based cryptography and encryption.
3. Data owner only can modify access policy.
4. Fast encryption, outsourced decryption and user revocation.

8. Modules

8.1 Data Owner

Data owner should be free to upload their files to the concern attribute. The system must identify each file with an automatically generated file Id, for future reference. System generates secret code and sent to data owner email and that secret code is required to upload file. Data owner should be allowed to check the status of their file, by using the unique file Id provided by the system. The system must display the file along with the details to the data owner, after uploading the file.

8.2 Data User

The data user should be able to see the uploaded files, which are uploaded by the data owner to specified attribute data user only. Data user can download files by sending key request if attribute authority send key to data user then and then data user can download files. Data user can check there key request status. A password protection with secure mode option is provided to guard from unauthorized access to database.

8.3 Attribute Authority

Attribute Authority can send response to key request coming from data user to download file. Attribute authority is mainly working on key management.

8.4 Proxy Server

Proxy server is a server who can encrypt and decrypt files. AES Asymmetric Encryption Standards is used for encryption and decryption.

8.4 Admin

Admin is a super user who has access of everything. Admin can manage users of the system.

9. System design

Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm and area is the first step in the development phase for any engineered product or system. The designer's goal is to produce a model or representation of an entity that will later be built. Beginning, once system requirement have been specified and analyzed, design is the first of the three technical activities - design, code and test that is required to build and verify software.

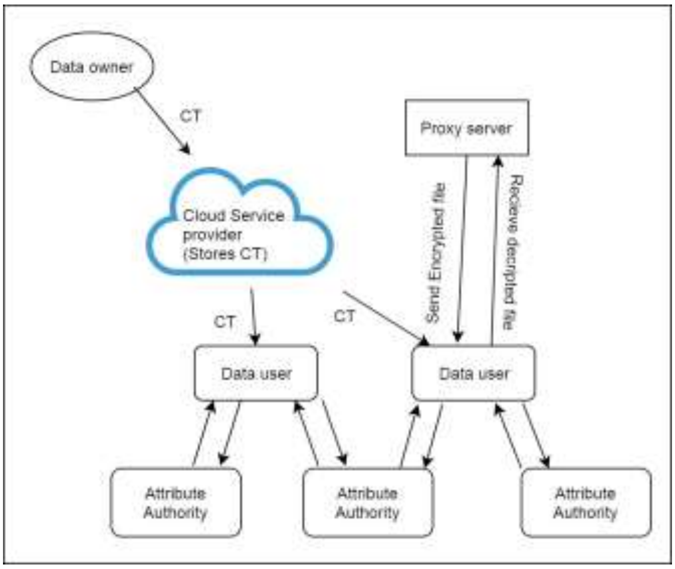

Fig -2: Proposed System design

10. CONCLUSIONS

Encryption mechanisms based on user identities and attributes hold a great promise for changing scenarios of computing, namely cloud computing and ubiquitous computing. These schemes relate a key with a set of attributes and thus alleviate the problem of key generation and distribution of PKI. Also, the concepts of such schemes can be used to further design trust and security y mechanisms for data storage in cloud.

In this paper we build a CPABE scheme in prime order. As pointed out by the proof of the scheme is in the generic group model using random oracles. The reason for using prime order groups is that the schemes are efficient with faster group operations. Our construction can be used to design a scheme in Composite order group, which though inefficient, rests on stronger notions of security in the dual system encryption model.

REFERENCES

[1] N. Attrapadung and H. Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278– 300. Springer, 2009.

[2] N. Attrapadung and H. Imai. Conjunctive broadcast and attribute-based encryption. In Pairing-Based Cryptography-Pairing 2009: Third International Conference Palo Alto, CA, USA, August 12-14, 2009 Proceedings, volume 5671, page 248. Springer Science & Business Media, 2009.

[3] N. Balani and S. Ruj. Temporal access control with user revocation for cloud data. In 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing, China, September 24-26, 2014, pages 336–343, 2014.

[4] A. Beimel. Secure schemes for secret sharing and key distribution. Ph.D. Thesis, Israel Institute of Technolgy, Technion, Haifa, Israel, 1996.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pages 321–334. IEEE Computer Society, 2007.

[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In Proceedings of the 15th ACM conference on Computer and communications security, pages 417–426. ACM, 2008.

[7] R. Canetti, H. Krawczyk, and J. B. Nielsen. Relaxing chosen-ciphertext security. In D. Boneh, editor, Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 565–582. Springer, 2003.

[8] M. Chase. Multi-authority attribute based encryption. In Proceedings of Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007 [8], pages 515– 534.

[9] M. Chase and S. S. M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009 [9], pages 121–130.