An Efficient Approach for Data Outsourcing using Attribute based Encryption

R. Aruna[1] R. Bhuvaneswari[2] R. Anbarasu[3]
[1]M.E – CSE Selvam College of Technology, Namakkal
[2, 3]Assistant Professor Selvam College of Technology, Namakkal

Abstract— A distributed system is a collection of autonomous computers linked by a computer network that appear to the users of the system as a single computer. In a large distributed system, security is provided by the use of cryptographic techniques such as key generation. It has a major role in solving Computational problems. Data outsourcing in a distributed system represents that a data owner outsource the data to the service provider. Data outsourcing require flexible access control policies to enforce authorizing key policies and maintaining key generating policy updates are the important issues in distributed system. A new approach Cipher text policy attribute based encryption (CP-ABE) system is implemented for key generation, Cipher text is associated with an access structure, while the secret keys are labeled with a set of attributes. Therefore access control mechanism enforces security policies with efficient attribute and user revocation capabilities. CP-ABE provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text. Further multiple service providers are used in a system and data is distributed among them. In CP-ABE fine grained access control can be achieved by dual encryption mechanism that is used to maintain the data. So computation overhead is reduced, it is used to securely manage the outsourced data.

I. INTRODUCTION

Modern data outsourcing systems require flexible access control approaches. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles. The data outsourcing scenario challenges the approaches of traditional access control architectures such as reference monitor, where a trusted server is in charge of defining and enforcing access control policies. This assumption no longer holds in modern data outsourcing systems, because users want to be able to share private contents with a group of people they selected and to define some access policy and enforce it on the contents. Thus, it is desirable to put the access policy decisions in the hands of the data owners. Recently proposed access control models, such as attribute-based access control; define access control policies based on different attributes of the requester, environment, or the data object. In addition, the current trend of storage outsourcing requires increased protection of data including access control methods that are cryptographically enforced.

The concept of attribute-based encryption (ABE) is a promising approach that fulfils these requirements. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. However, the problem of applying the ABE to the data outsourcing architecture introduces several challenges with regard to the attribute and user revocation. The revocation issue is even more difficult especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. It may result in bottleneck during rekeying procedure or security degradation in the system. Thus, in this study, we will attempt to solve these problems in attribute-based data access control using CP-ABE for data outsourcing systems.

II. RELATED WORK

ABE comes in two flavour's called key-policy ABE (KP-ABE) and cipher text-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into user's keys; while in CP-ABE, the attributes are used to describe a user's credential, and an encryptor determines a policy on who can decrypt the data. CP-ABE is more appropriate to the data outsourcing architecture than KPABE because it enables data owners to choose an access structure on attributes and to encrypt data to be outsourced under the access structure via encrypting with the corresponding public attributes. Attribute Revocation Recently, several attribute revocable ABE schemes have been proposed. They realize revocation by revoking attribute itself using timed rekeying mechanism, which is implemented by setting expiration time on each attribute. We call this a coarse-grained revocation because the immediate rekeying on any member change could not be possible. Indeed, these approaches have two main problems. First problem is the security degradation in terms of the backward and forward secrecy. An attribute is supposed to be shared by a group of users in the ABE systems by nature. Then, it is a considerable scenario that membership may change frequently in the group that shares an attribute.

A. *User Revocation*

Recently, the importance of user revocation has been taken notice of in many practical ABE-based systems. The user revocation is an essential mechanism in many group-based applications including ABE systems, because users may change their attributes frequently in practice. The fine-grained user-level revocation can be done by using ABE that supports negative clauses, proposed in. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). The previous user-revocable schemes also have a limitation with regard to the availability.

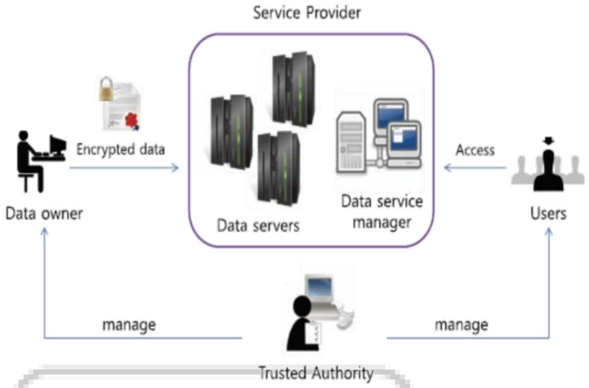

Fig.1: Data outsourcing Architecture

Fig.1, this is related to the granularity of the user access control between attribute level or system-level revocation. When a user is revoked even from a single attribute group in the previous schemes, he loses all the access rights to the data sharing system. That is, the previous schemes realized user revocation on system-level, which means that when a user is revoked even from a single attribute group, he is destined to be revoked from the whole system. Such a scenario is not as desirable as the attribute-level user access control in many practical data outsourcing scenarios, although they realized immediate user revocation. However, in this scheme, the data owner should take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation. This scheme is not applicable to the data outsourcing architecture, because the data owners will no longer be directly in control of data distribution after outsourcing their data to the external data server.

B. *Cipher text-Policy Attribute-Based Encryption*

In Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access policy over attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed.

C. *Classical access control architectures*

The reference monitor typically represents the core component of any access control system. Fig.2 policy changes and data updates at a limited cost. The realization of cryptographic access protection. Data dissemination has to correctly manage. An efficient management of policy updates. Outsourced architecture introduces several challenges. Impose strong constraints on the way sensitive information can be managed Difficult to manage data in a distributed setting.

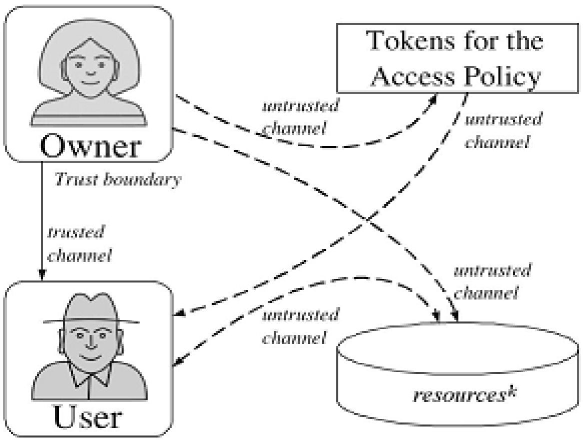

Fig.2: Architecture of a system using a reference monitor

III. PROPOSED SYSTEM

The proposed system implements the entire existing concept, a new approach Cipher text-Policy Attribute-Based Encryption with User Revocation is carried out. The proposed system adapts a dual encryption approach to overcome the user access control problem in attribute-based encryption system. Cipher text is associated with an access structure, while the secret keys are labeled with a set of attributes. Therefore access control mechanism enforces security policies with efficient attribute and user revocation capabilities. CP-ABE provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text. Revocation corresponds to the withholding or withdrawal of consent. It is manifested in its simplest form as deletion of data, although there are many variations of revocation, as listed below:

A. *No Revocation at All*

Personal data remains static, and once it has been disclosed, it is either physically impossible to revoke (how could one ever revoke reputation) or prohibited for various reasons (e.g. law-enforcement, data from police’s DNA database).

B. *Deletion*

Data are completely erased and cannot be retrieved or reconstituted in any way.

C. *Revocation of Permissions to Process Data*

Data subjects withdraw consent that would enable an enterprise to process or analyze their personal data for a specified purpose.

D. *Revocation of Permissions for Third Party Dissemination*

Data subjects withdraw consent that would enable an enterprise to disclose information to a third party. In addition, multiple service providers are included and data is distributed among them. User privileges may be varying for data maintained by different service providers. This requires different kind of encryption mechanisms in data maintained by different service providers and so computations overhead is reduced and securely maintain the outsourced data.

IV. IMPLEMENTATION

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 fig.3, they present a system for realizing complex access control on encrypted data that they call Cipher text-Policy Attribute-Based Encryption.

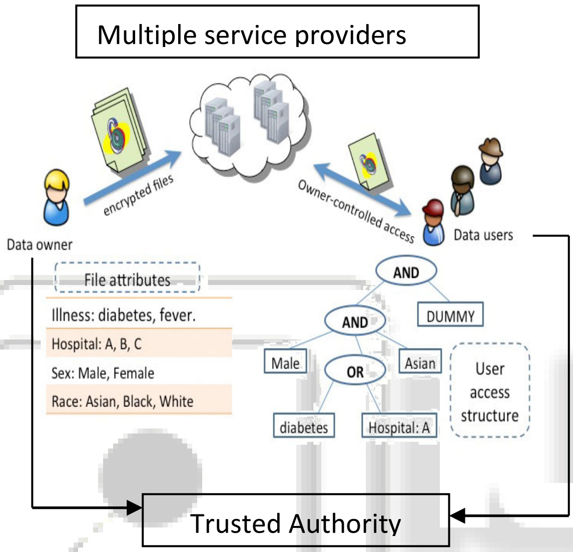

Fig.3.Architrecture of attribute based encryption

Fig.4 let T be a tree representing an access structure. Each nonleaf node of the tree represents a threshold gate. Leaf node x in the tree represents the parent of the node x in the tree. The children of every node are numbered from 1 to num. The function index δxp returns such a number associated with the node x updates. If numx is the number of children of a node x and kx is its threshold value, then 0 _ kx _ numx. Each leaf node x of the tree is described by an attribute and a threshold value kx = 1. x denotes the attribute associated with the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

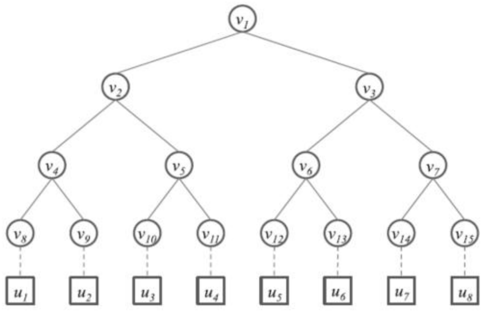

Fig .4: KEK Tree for attribute group key distribution

V. CONCLUSION AND FUTURE WORK

Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. This System proposes a cryptographic approach to enforce a fine-grained access control on the outsourced data that is dual encryption protocol exploiting the combined features of the cipher text-policy attribute-based encryption and group key management algorithm. The proposed scheme allows a data owner to define the access control policy and enforce it on his outsourced data. It also features a mechanism that enables more fine-grained access control with efficient attribute and user revocation capability. It is efficient and scalable to securely manage the outsourced data. Furthermore, each authority can join or leave the system freely without the need of reinitializing the system. The data integrity in multiple copies of same data base not consider.The error situation can be recovered if there is any mismatch. The web site and database can be hosted in real environment during the implementation.

REFERENCES

[1]N. P. Smart. (2003) “Access control using pairing based cryptography,” in The Cryptographers’ Track at the RSA Conference - CT-RSA’03, vol. 2612 of LNCS, pp. 111–121

[2]J. Bethencourt, A. Sahai, and B. Waters. (2007)“Ciphertext-policy attribute-based encryption,” in Proceedings: IEEE Symposium on Security and Privacy (S & P’07), (Oakland, California, USA), pp. 321– 34, IEEE, May 20-23

[3]A. Sahai and B. Waters. (2005) “Fuzzy identity-based encryption,” in Proceedings: Advances in Cryptology - EUROCRYPT’05 (R. Cramer, ed.), vol. 3494 of Lecture Notes in Computer Science, (Aarhus, Denmark), pp. 457–473, Springer, May 22-26

[4]M. Chase (2007) “Multi-authority attribute based encryption” in Proceedings: Theory of Cryptography Conference-TCC’07 (S. P. Vadhan, ed.), vol. 4392 of Lecture Notes in Computer Science, (Amsterdam, The Netherlands), pp. 515–534, Springer, February

[5]D. Boneh and M. K. Franklin. (2001) “Identity-based encryption from the weil pairing,” in Proceedings: Advances in Cryptology-CRYPTO’01 (J. Kilian, ed.), vol. 2139 of Lecture Notes in Computer Science, (Santa Barbara, California, USA), pp. 213–229, Springer, August 19-23

[6]V. Goyal, O. Pandey, A. Sahai, and B. Waters. (2006) “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings: ACM Conference on Computer and Communications Security-CCS’06 (A. Juels, R. N. Wright, and S. D. C. di Vimercati, eds.), (Alexandria, VA, USA), pp. 89–98, ACM, October 30- November

[7]R. Ostrovsky, A. Sahai, and B. Waters. (2007) “Attribute- based encryption with non-monotonic access structures,” in Proceedings: ACM Conference on Computer and Communications Security-CCS’07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 195–203, ACM, October 28-31

[8]L. Cheung and C. Newport. (2007) “Provably secure Ciphertext policy abe,” in Proceedings: ACM Conference on Computer and Communications Security - CCS’07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 456–465, ACM, October 28-31

[9]J. Hur and D. K. Noh. (2011) “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221

[10]R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. (2009) “Persona: An Online Social Network with User-Defined Privacy,” Proc. ACM SIGCOMM ’09, Aug.