ISSN 2395-1621

Attribute Based Encryption & Decryption on Cloud Computing

[#1]Inkar Akash, [#2]Admane Balaji, [#3]Kamble Poonam, [#4]Prof. V. S. Wadne

[1]akashinkar777@gmail.com
[2]balajiadmane9823@gmail.com
[3]poonamk12345@gmail.com

[#1234]Department of Computer Engineering

JSPM's ICOER, Pune.

ABSTRACT

Ciphertext policy attribute-based encryption (CP-ABE) is a promising cryptographic technique for fine-grained access control of outsourced data in the cloud. However, some drawbacks of key management hinder the popularity of its application. One drawback in urgent need of solution is the key escrow problem. We indicate that front-end devices of clients like smart phones generally have limited privacy protection, so if private keys are entirely held by them, clients risk key exposure that is hardly noticed but inherently existed in previous research. Furthermore, enormous client decryption overhead limits the practical use of ABE. In this work, we propose a collaborative key management protocol in CP-ABE (CKM-CP-ABE). Our construction realizes distributed generation, issue and storage of private keys without adding any extra infrastructure. A fine-grained and immediate attribute revocation is provided for key update. The proposed collaborative mechanism effectively solves not only key escrow problem but also key exposure. Meanwhile, it helps markedly reduce client decryption overhead. A comparison with other representative CP-ABE schemes demonstrates that our scheme has somewhat better performance in terms of cloud-based outsourced data sharing on mobile devices. Finally, we provide proof of security for the proposed protocol.

ARTICLE INFO

Article History

Received: 13th December 2017

Received in revised form :

13th December 2017

Accepted: 15th December 2017

Published online :

15th December 2017

Keywords: Cloud data sharing, CP-ABE, Key management, Security, Efficiency.

I. INTRODUCTION

Cloud computing, is trending in all sectors like governments, non-profits or small businesses and even unto fortune 500 companies. However, as organizations continue to take benefits of cloud services, they must consider how the introduction of cloud services affects their privacy and security.

The motivation of the cloud repository system is as follows:

1. Providing security to the data stored on the cloud from unauthorized access, intruders, employees of the enterprise, and even from the cloud service providers.
2. Identity Management to avoid serious crimes involving identity theft.
3. Increasing the efficiency of the cloud storage system by encrypting files with distinct keys.
4. Sharing multiple files securely with the registered users in the system.
5. Restricting access control levels for private and public files.
6. Focus on the decryption of the distinct set of cipher data by using Access key.
7. Decrease the amount of cost while decrypting the cipher data from the cloud storage system.

Overview:

Cloud computing is a computing paradigm, where a large pool of systems are connected in

private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption."

II. LITERATURE SURVEY

The literature survey that containing study of different schemes available in Attribute Based encryption(ABE).That are KP-ABE,CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, ABE and MABE. Also include advantage ,disadvantage and a comparison table of each scheme based on fine grained access control, efficiency, computational overhead and collusion resistant.

A. Attribute based encryption (ABE):

An attribute based encryption scheme introduced by Sahai and Waters in 2005 and the goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. In which the secretkey of a user and the ciphertext are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. Decryption is only possible when the number of matching is at least a threshold value d. Collusion-resistance is crucial security feature of Attribute-BasedEncryption .An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. 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.

B. Key Policy Attribute Based Encryption(KP-ABE):

It is the modified form of classical model of ABE. 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. To reflect the access tree Structure the secret key of the user is defined. Ciphertexts are labelled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.

III. PROPOSED SYSTEM

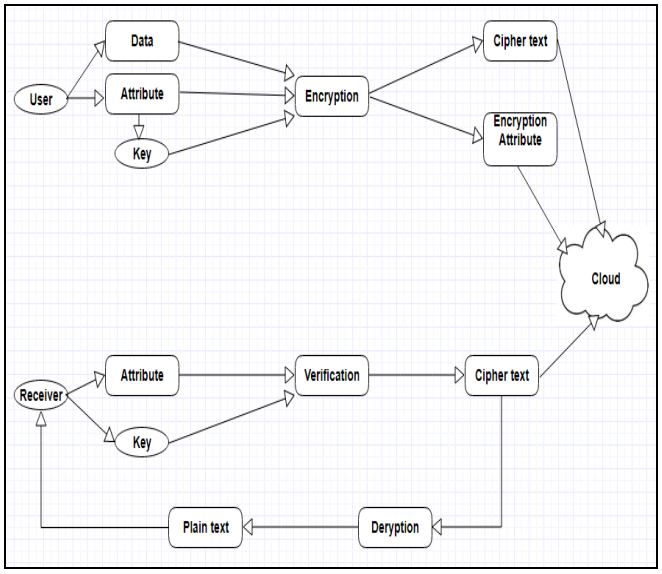

Fig 1. System architecture

Setup : This algorithm takes as input a security parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encrypt : This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT. Key-Gen : This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Decrypt : This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

IV. CONCLUSION

In this paper, we analyse different attribute-based encryption schemes: ABE. Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance the sensitive data, and moreover towards the anonymity of the data owner. Our scheme also enables dynamic modification of access policies o supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

REFERENCES

[1] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[2] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multiauthority attribute-based encryption with honest-but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3, 2012.

[3] V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006}

[4] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[5] Muller, S. Katzenbeisser, and C.Eckert, "Distributed attribute-based encryption," in Proceedings of ICISC, pp. 20{36, 2008.

[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. "Secure attribute-based systems". In Proceedings of the 13th ACM conference on Computer and communications security, pages 99{112. ACM Press New York, NY, USA, 2006.

[7] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[8] R. Ostrovsky and B. Waters. "Attribute based encryption with nonmonotonic access structures".In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY, USA,2007.

[9] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473

