IJRRECS/August 2015/Volume-3/Issue-8/4520-4524 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A SECURE APPROACH FOR ACCESS CONTROL OF STORED ENCRYPTED DATA IN CLOUD SYSTEM

Rajam Mallesh[1], Dr.Vaka Murali Mohan[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

[2]Professor & HOD, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

ABSTRACT:

Attribute-based encryption is a novel mechanism of public key basis encryption which is one-to-many and enables access control on encrypted data by means of access policies connected with private keys. We modify the actual representation of attribute-based encryption by means of outsourced decryption to permit for verifiability of transformations. We study a novel prerequisite of attribute-based encryption by outsourced decryption that is Verifiability which assures that user can resourcefully make sure when transformation is done accurately. For assessment of performance of attribute-based encryption scheme by means of verifiable outsourced decryption, we put into practice cipher text-policy basis attribute encryption scheme by means of verifiable outsourced decryption.

Keywords: Attribute-based encryption, Cipher text-policy, Decryption, Verifiability, Access control.

1. INTRODUCTION:

Attribute-based encryption is an encryption technique that allows encryption and decryption of data based on user attributes. There are several drawbacks for most of the traditional schemes of attribute-based encryption and among them one of the drawbacks is that decryption is costly for resource restricted devices because of pairing operations which are necessary to decrypt a cipher-text that grows with difficulty of access policy [1]. In recent times, Green et al. projected a solution to this problem by means of introduction of

attribute-based encryption by means of outsourced decryption that eliminates decryption transparency for users to a great extent. Security regarding attribute-based encryption system by means of outsourced decryption makes sure that adversary will not learn anything regarding encrypted message; on the other hand, it does not assurance accuracy of transformation made by the cloud. Attribute-based encryption is of two kinds such as key-policy as well as cipher text-policy attribute-based encryption. In cipher text-policy basis attribute encryption every cipher-text is connected by means of an access policy on attributes, and each user private key is linked by a set of attributes. In our work we make a consideration of a novel requirement of attribute-based encryption by outsourced decryption. Verifiability assures that user can resourcefully make sure when transformation is done accurately.

2. METHODOLOGY:

An efficient application of attribute-based encryption is access control of encrypted information that is stored in cloud, by means of access polices related with private keys. In our work we make a modification of actual representation of attribute-based encryption by means of outsourced decryption to permit for verifiability of transformations [2]. In existing mechanism of attribute-based encryption decryption is costly for resource restricted devices because of pairing operations which are necessary to decrypt a cipher-text that grows with difficulty of access policy. Later projected a solution was proposed by means of introduction of attribute-based encryption by means of outsourced decryption that eliminates decryption transparency for users to a great extent. In this system user provides an untrustworthy server, such as cloud service provider, by means of a transformation key that allows cloud to alter any attribute-based encryption cipher-text that is satisfied by access policy into an effortless cipher-text. It incurs a small computational transparency for user to get better plaintext from transformed cipher-text. We make a consideration of a novel requirement of attribute-based encryption by outsourced decryption that is Verifiability which assures that user can resourcefully make sure when transformation is done accurately. To achieve verifiability, we need to alter the model of cipher text-policy basis attribute encryption with outsourced decryption. The security property of

attribute-based encryption system by means of outsourced decryption assurance that an adversary is unable to find out anything regarding encrypted message; on the other hand, the system provides no assurance on accuracy of the transformation that is made by cloud server. For estimation of performance of our attribute-based encryption scheme by means of verifiable outsourced decryption, we put into practice cipher text-policy basis attribute encryption scheme by means of verifiable outsourced decryption.

3. AN OVERVIEW OF PROPOSED SYSTEM:

In cloud computing situation, providers of cloud service might have tough economic incentives to return inaccurate answers, when such answers necessitate less work and are not likely to be noticed by users. Attribute-basis encryption is technique that permits encryption and decryption of data on basis of user attributes [3][4]. In the actual model, a cipher text-policy basis attribute encryption method by means of outsourced decryption consists of five algorithms. A trustworthy party make use of the algorithm to produce public parameters as well as a master secret key, and make use produce a private key as well as transformation key for user. Consideration as input transformation key when specified by a user and a cipher-text, cloud can make use of algorithm to change cipher-text into an effortless cipher-text when user attribute convince access structure that is connected with cipher text; then user make use of algorithm to get better plaintext from transformed cipher text. By Green etal., input to algorithm comprise only private key of user and transformed cipher text, however does not comprise new cipher-text. Due to omission of actual cipher text, it is not likely to construct a cipher text-policy basis attribute encryption by verifiable outsourced decryption. A malevolent cloud might restore the cipher text it suppose to transform by a cipher text of various messages, and subsequently transform latter into an easy cipher text by means of its transformation key. The user cannot notice malicious actions of cloud while input to algorithm does not comprise original cipher text that is necessary to be transformed. To attain verifiability, we need to change the model of cipher text-policy basis attribute encryption with outsourced decryption. We make a modification of actual representation of attribute-based encryption by means of outsourced

decryption to permit for verifiability of transformations. In our model at the setup stage of our projected attribute based encryption by verifiable outsourced decryption system, user can just begin a normal attribute based encryption devoid of outsourced decryption. Later user can produce transformation key when he needs to outsource decryption, devoid of having to reset up of complete system. When trustworthy party is accountable for production of transformation keys, user is necessary to reinitialize system in support of outsourced decryption. While conventional view of security against adaptive chosen-cipher-text attacks does not permit any bit of cipher text to be changed, we implement a relaxation because of Canetti et al. known as replayable chosen-cipher-text attacks security that allows alterations to cipher-text provided they cannot alter fundamental message in a significant means. Replayable chosen-cipher-text attacks security in support of cipher text-policy basis attribute encryption with outsourced decryption is explained as a game among challenger as well as an adversary. One tough idea of verifiability is that, even when trustworthy party who setups system is malevolent, user still can verify on accuracy of transformation done by cloud [5][6]. Adversaries produce system public parameters as well as master secret key. Nevertheless, it is tricky to build a cipher text-policy basis attribute encryption scheme by means of outsourced decryption which is provable in stronger model, while most of the traditional techniques of verifiable security need to produce system's public parameters highly by challenger.

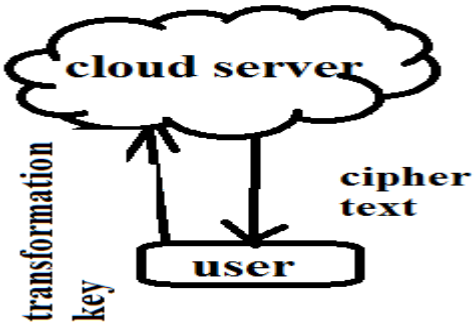

Fig1: An overview of proposed system.

4. CONCLUSION:

In traditional mechanisms of attribute-basis encryption decryption is expensive for resource restricted devices because of pairing operations which are necessary to decrypt a cipher-text that grows with difficulty of access policy. A solution was proposed by means of introduction of attribute-based encryption by means of outsourced decryption that eliminates decryption transparency for users. In our work we consider a novel necessity of

attribute-based encryption by outsourced decryption. Verifiability guarantees that user can efficiently make sure when transformation is done accurately. For assessment of performance of attribute-based encryption method by means of verifiable outsourced decryption, we practise cipher text-policy basis attribute encryption scheme by means of verifiable outsourced decryption. In this system user offer an unreliable server, such as cloud service provider, by means of a transformation key that allows cloud to alter any attribute-based encryption cipher-text that is satisfied by access policy into an effortless cipher-text.

REFERENCES

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. EUROCRYPT, 1998, pp. 127–144.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. NDSS, San Diego, CA, USA, 2005.

[3] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," Ph.D. dissertation, Israel Inst. of Technology, Technion City, Haifa, Israel, 1996.

[4] M. Green, A. Akinyele, and M. Rushanan, Libfenc: The Functional Encryption Library.

[5] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Proc. CRYPTO, 2010, pp. 465–482.

[6] K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in Proc. CRYPTO, 2010, pp. 483–501.