IJRRECS/August 2014/Volume-2/Issue-8/3056-3060 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

ADVANCE TOWARDS SUPERIOR ENTRUSTMENT OF COMPUTATION

B.Sunitha[1], K.Nagi Reddy[2]

[1]M.Tech Student, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, T.S, India

ABSTRACT:

There exist quite a lot of significant attribute based encryption schemes where decryption algorithm simply necessitates a steady number of pairing computations. Attribute based encryption system with secure outsourced decryption does not essentially assurance verifiability specifically exactness of transformation done by cloud server. To assess performance of attribute based encryption scheme with confirmable outsourced decryption, we put into practice cipher text-policy attribute based encryption system with confirmable outsourced decryption. In attribute based encryption with outsourced decryption, a user make available cloud by means of a transformation key that permit cloud to interpret an attribute based encryption cipher text on message into an undemanding ciphertext. We put forward a new cipher text-policy attribute based encryption system utilizing Waters' cipher text-policy attribute based encryption which is confirmed to be selectively CPA-secure. Concrete attribute based encryption schemes by outsourced decryption were suggested and in these schemes, a user makes available an untrusted server, say a proxy functional by a cloud service provider.

Keywords: Attribute based encryption, Cloud service provider, Cipher text-policy, Proxy system.

1. INTRODUCTION:

In environment of cloud computing, providers of cloud service might contain well-built financial incentives to return erroneous answers, if such answers necessitate less effort and are improbable to

be noticed by users [1]. Attribute based encryption as shown in fig1 is a novel public key based one-to-many encryption that facilitates access control on access policies of encrypted data. The most important effectiveness drawbacks of most existing schemes of attribute based encryption is that decryption is high-priced for resource-limited devices due to pairing procedures, along with number of pairing operations necessary to decrypt a cipher text grows with difficulty of access policy. Security property of attribute based encryption system with outsourced decryption assurance that an adversary be not competent to find out anything concerning the encrypted message; on the other hand, the system provides no assurance on the accuracy of transformation completed by cloud server [2][3]. User is capable to decrypt a cipher text as long as set of attributes connected with user's private key convince access policy connected with cipher text. There are two kinds of attribute based encryption systems such as: key-policy attribute based encryption as well as cipher text-policy attribute based encryption. In a cipher text-policy attribute based encryption, each ciphertext is connected by an access policy on attributes, and each private key of user is connected with a set of attributes. In attribute based encryption with outsourced decryption, a user make available cloud by means of a transformation key that permit cloud to interpret an attribute based encryption cipher text on message into an undemanding ciphertext [4][5]. In a key-policy attribute based encryption, the roles of attribute set as well as an access policy are swapped from cipher text-policy attribute based encryption: attributes sets are employed to annotate cipher texts as well as access polices over these attributes are connected with users' private keys. To assess performance of attribute based encryption scheme with confirmable outsourced decryption, we put into practice cipher text-policy attribute based encryption system with confirmable outsourced decryption and carried out experiments on ARM-based mobile device and an Intel-core personal computer to form a mobile user as well as a proxy, respectively.

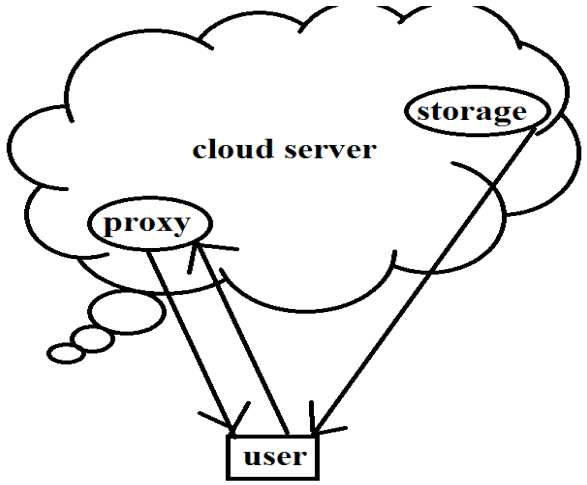

Fig1: An overview of attribute based encryption system through outsourced decryption.

2. METHODOLOGY:

In distributed situation with un-trusted servers, for instance the cloud, numerous applications require mechanisms for intricate access-control on encrypted information. User is capable to decrypt a cipher text as long as set of attributes connected with user's private key convince access policy connected with cipher text. Imagine a cloud based system of electronic medical record in which patients' records are confined by means of attribute based encryption schemes by means of outsourced decryption and are accumulated in cloud [6]. Specified a transformed cipher text from proxy, doctor can understand a patient's medical record by performing an effortless measure of computation. To access patients' records on mobile phone, a doctor produces and entrust a transformation key to a proxy in cloud for outsourced decryption [7][8]. If no verification of correctness of transformation is assured, however, system might run into problems such as for rationale of saving computing expenditure, proxy could return medical record transformed earlier for similar doctor; due to malicious attack, proxy could convey the medical record of an additional patient or a file of accurate form but carrying erroneous information. Attribute based encryption system with secure outsourced decryption does not essentially assurance verifiability specifically exactness of transformation done by cloud server. The outcome of treating patient based on erroneous information could be extremely serious or even terrible. We put forward a new cipher text-policy attribute based encryption system utilizing Waters' cipher text-policy attribute based encryption which is confirmed to be selectively CPA-secure. Security ensures that an adversary not is capable to discover anything concerning encrypted message and verifiability permit a user to ensure on accuracy of transformation done by cloud.

3. AN OVERVIEW OF PROPOSED SYSTEM:

At expenditure of security, only confirmed in a weak model there exist quite a lot of significant attribute based encryption schemes where decryption algorithm simply necessitate a steady number of pairing computations. Attribute based encryption is a novel public key based one-to-many encryption that facilitates access control on access policies of encrypted data. Based on the existing attribute based encryption schemes, concrete attribute based encryption schemes by outsourced decryption were suggested and in these schemes, a user makes available an untrusted server, say a proxy functional by a cloud service provider, by means of a transformation key that permit the latter to translate any attribute based encryption cipher text satisfied by user's attributes or else access policy into an effortless cipher text, and it merely incurs a minute transparency for user to recuperate plaintext from transformed cipher text. In attribute based encryption with outsourced decryption, a user make available cloud by means of a transformation key that permit cloud to interpret an attribute based encryption cipher text on message into a undemanding ciphertext. When using paring delegation in decryption of attribute- based encryption cipher texts, quantity of computation of client is proportional to extent of access policy. We put forward a new cipher text-policy attribute based encryption system utilizing Waters' cipher text-policy attribute based encryption which is confirmed to be selectively CPA-secure. We put forward a cipher text-policy attribute based encryption scheme with outsourced decryption and confirm that it is selectively CPA-secure and confirmable in standard representation.

4. CONCLUSION:

Attribute based encryption is a novel public key based one-to-many encryption that facilitates access control on access policies of encrypted data. Attribute based encryption system with secure outsourced decryption does not essentially assurance verifiability specifically exactness of transformation done by cloud server. The most important effectiveness drawbacks of most existing schemes of attribute based encryption is that decryption is high-priced for resource-limited devices due to pairing procedures, along with number of pairing operations necessary to decrypt a cipher text grows with difficulty of access policy. In a

cipher text-policy attribute based encryption, each ciphertext is connected by an access policy on attributes, and each private key of user is connected with a set of attributes. To assess performance of attribute based encryption scheme with confirmable outsourced decryption, we put into practice cipher text-policy attribute based encryption system with confirmable outsourced decryption. We put forward a new cipher text-policy attribute based encryption system utilizing Waters' cipher text-policy attribute based encryption which is confirmed to be selectively CPA-secure. Based on the existing attribute based encryption schemes, concrete attribute based encryption schemes by outsourced decryption were suggested and in these schemes, a user makes available an untrusted server, say a proxy functional by a cloud service provider. We put forward a cipher text-policy attribute based encryption scheme with outsourced decryption and confirm that it is selectively CPA-secure and confirmable in standard representation. When using paring delegation in decryption of attribute- based encryption cipher texts, quantity of computation of client is proportional to extent of access policy.

REFERENCES

[1] S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich, "Succinct functional encryption and applications: Reusable garbled circuits and beyond," IACR Cryptology ePrint Archive, vol. 2012, p. 733, 2012.

[2] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, "Secure delegation of elliptic-curve pairing," in Proc. CARDIS, 2010, pp. 24–35.

[3] B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairing computation," IACR Cryptology ePrint Archive, vol. 2005, p. 259, 2005.

[4] P. P. Tsang, S. S. M. Chow, and S. W. Smith, "Batch pairing delegation," in Proc. IWSEC, 2007, pp. 74–90.

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

[6] 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.

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

[8] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. EUROCRYPT, 2011, pp. 568–588.