IJRRECS/November 2015/Volume-3/Issue-11/4804-4809 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFECTIVE ENCRYPTION APPROACH FOR SHARING OF DATA IN CLOUD SYSTEMS

E.Chandrakala[1], M.Rani[2]

[1]M.Tech Student, Dept of CSE, Sri Mittapalli Institute of Technology for Women, Guntur, A.P, India

[2]Assistant Professor, Dept of CSE, Sri Mittapalli Institute of Technology for Women, Guntur, A.P, India

ABSTRACT:

In the recent times, process of Attribute basis encryption was proposed that permits encryption of each data item that is on the basis of access control policy which is valid to data. In spite of latest advancements that are made in functioning methods, computational costs that are necessary for pairing are significantly high when compared to standard operations costs. For managing of the issues of performance as well as security issues, in our work we propose a Mediated certificate-less public key encryption approach devoid of usage of pairing operations. The proposed public key encryptions of existing works are ineffective due to practice of costly pairing operations. We put forward a mediated certificate-less encryption system devoid of pairing operations intended for efficient sharing of sensitive information within public clouds. The proposed public key encryption will resolve problem of key escrow within identity based encryption as well as certificate revocation difficulty within public key cryptography. Our system will reduce computational transparency by means of using a pairing-free approach.

Keywords: Attribute basis encryption, Public key cryptography, Mediated certificate-less public key encryption, Key escrow, Identity based encryption.

1. INTRODUCTION:

For assuring of confidentiality of important data that is stored up within public clouds, generally accepted approach is encryption of data previous to uploading into cloud system. While the system of cloud does not make out the keys that are used for data encryption, data privacy from the cloud is guaranteed [1]. As several organizations are necessary to implement fine-grained access control towards data, mechanism of encryption has to support fine-grained encryption process which is based on access control. Besides containing the problem of key escrow, Attribute basis encryption contains revocation difficulty as private keys that are specified to existing users have to be updated when a user is revoked. For handling the issue of key escrow problem a novel cryptosystem known as Certificate-less Public Key Cryptography was proposed. Later an approach of Certificate-less Proxy Re-Encryption for protected data sharing within public cloud environments was proposed. Mediated certificate-less public key encryptions of existing works are ineffective due to practice of costly pairing operations. For addressing the issues of performance as well as security issues, in our work we propose a Mediated certificate-less public key encryption approach devoid of usage of pairing operations. The proposed Mediated certificate-less public key encryption will resolve problem of key escrow within identity based encryption as well as certificate revocation difficulty within public key cryptography [2]. The proposed system was applied to build a realistic solution to the difficulty of sharing sensitive data within public clouds. Major benefit of our approach when compared to existing approaches is that key generation center, which is entity responsible for generation of keys will exist in public cloud hence it will simplify various key management for organizations.

2. METHODOLOGY:

Although key derivation-based methods will decrease keys to be managed, mechanisms of symmetric key basis generally have the difficulty of extreme costs for key management. In our work we deal with shortcomings of earlier approaches and suggest a mediated certificate-less encryption system devoid of pairing operations intended for efficient sharing of sensitive information within public clouds and that does not make use of pairing operations. For handling key escrow

problem a novel cryptosystem known as Certificate-less Public Key Cryptography was proposed. As most of these methods are based on bilinear pairings, they are costly. Proposal of Mediated certificate-less public key encryption of existing works are ineffective due to practice of costly pairing operations. For addressing the issues of performance as well as security issues, in our work we propose a Mediated certificate-less public key encryption approach devoid of usage of pairing operations. Our system will reduce computational transparency by means of using a pairing-free approach. On our proposed approach, we recommend a novel approach to guarantee data privacy that is stored within public clouds while put into effect needs of access control. Computation costs intended for decryption at users are decreased as semi-trustworthy security mediator will decrypt encrypted data earlier than users decrypt. When compared to symmetric key based methods, our proposed approach will resourcefully manage keys as well as user revocations. In symmetric key systems, users manage several keys equivalent to at least logarithm of several users, whereas in our approach, each of the users needs to preserve its key pair [3]. Mediated certificate-less encryption system was proposed devoid of pairing operations intended for efficient sharing of sensitive information within public clouds. Mediated certificate-less encryption system was applied to build a realistic solution to the difficulty of sharing sensitive data within public clouds. The cloud is used as an effective storage in addition to key generation center. In our system, data owner will encrypt sensitive information by means of cloud produced user public keys on basis of access control policies and upload encrypted information towards cloud. On successful agreement, cloud will partially decrypt encrypted information for users who later decrypt partially decrypted information by means of their private keys. The content privacy as well as keys is preserved regarding cloud, since cloud cannot completely decrypt information. Consistent with access control policy, data owner will encrypt encryption key of symmetric data by means of proposed scheme and encrypt data items by means of symmetric encryption algorithm [4]. Major benefit of our approach when compared to existing approaches is that Key generation center, which is entity responsible for generation of keys will exist in public cloud hence it will simplify various key

management for organizations. The proposed Mediated certificate-less public key encryption will resolve problem of key escrow within identity based encryption as well as certificate revocation difficulty within public key cryptography.

3. AN OVERVIEW OF PROPOSED SYSTEM:

For extensive implementation of cloud storage services, storage model of public cloud have to solve significant issue of data privacy. Shared sensitive information has to be secured from unofficial accesses. Distinctive method supports access control on basis of fine-grained encryption encrypts various sets of data items to which same access control policy applies with dissimilar symmetric keys and provide users applicable keys. We deal with shortcomings of earlier approaches and suggest a mediated certificate-less encryption system devoid of pairing operations intended for efficient sharing of sensitive information within public clouds and that does not make use of pairing operations. The proposed public key encryption will resolve problem of key escrow within identity based encryption as well as certificate revocation difficulty within public key cryptography. Our system will decrease computational transparency by means of using a pairing-free approach and the system will resourcefully manage keys as well as user revocations. On our proposed approach of Mediated certificate-less public key encryption, we recommend a novel approach to guarantee data privacy that is stored within public clouds while put into effect needs of access control. Mediated certificate-less public key encryptions of existing works are ineffective due to practice of costly pairing operations. There are five entities in our scheme as shown in fig1 such as data owner, users, Security mediator, and Key generation center as well as storage service [5]. Security mediator, Key generation center as well as storage service are semi-trustworthy and exist in a public cloud. While these are not trustworthy for data confidentiality and keys, they are trustworthy for execution of protocols accurately. Consistent with access control policy, data owner will encrypt encryption key of symmetric data by means of Mediated certificate-less public key encryption scheme and encrypt data items by means of symmetric encryption algorithm. Later data owner will upload items of encrypted data and encrypted data encryption key towards cloud. Major benefit

of our approach when compared to existing approaches is that Key generation center, which is entity responsible for generation of keys will exist in public cloud hence it will simplify various key management for organizations. It is important to observe that when one will apply our basic mediated certificate-less public key encryption scheme towards cloud computing and when numerous users are approved to access same information, encryption costs at data owner will turn out to be relatively high. In such situation, data owner will encrypt same information encryption key numerous times, once for every user, by means of user's public keys. Mediated certificate-less encryption system was applied to build a realistic solution to the difficulty of sharing sensitive data within public clouds. The cloud is used as an effective storage in addition to key generation center. In our system, data owner will encrypt sensitive information by means of cloud produced user public keys on basis of access control policies and upload encrypted information towards cloud. Cloud will partially decrypt encrypted information for users who later decrypt partially decrypted information by means of their private keys. The content privacy as well as keys is preserved regarding cloud, since cloud cannot completely decrypt information. Our approach will permit one to contain most of key generation as well as management functionality that is deployed in untrustworthy cloud as our proposed system does not contain key escrowing problem and as a consequence key generation centre is not capable to study complete user private keys [6].

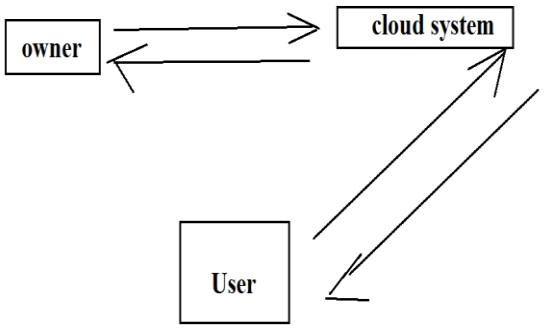

Fig1: an overview of certificate-less public key encryption approach.

4. CONCLUSION:

Several recent efforts were proposed to construct privacy preserving methods of access control by means of combining of oblivious transfer as well as anonymous credentials. Existing works of public key encryptions of are ineffective due to practice of costly pairing operations. For addressing performance as well as security issues, in our work we propose a Mediated certificate-less public key encryption approach devoid

of usage of pairing operations. We recommend a mediated certificate-less encryption system devoid of pairing operations intended for efficient sharing of sensitive information within public clouds. The projected public key encryption will resolve problem of key escrow within identity based encryption as well as certificate revocation difficulty within public key cryptography. Our system will decrease computational transparency by using a pairing-free approach. When compared to symmetric key based methods, our proposed approach will resourcefully manage keys as well as user revocations. Our proposed encryption system was applied to build a realistic solution to the difficulty of sharing sensitive data within public clouds.

REFERENCES

[1] E. Bertino and E. Ferrari. "Secure and selective dissemination of XML documents," ACM TISSEC, vol. 5, no. 3, pp. 290–331, 2002.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. 2007 IEEE Symp. SP, Taormina, Italy, pp. 321–334.

[3] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, Feb. 2004.

[4] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in Proc. 29th Int. Conf. VLDB, Berlin, Germany, 2003, pp. 898–909.

[5] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Knowl. Data Eng., vol. 25, no. 11, pp. 2602–2614, Sept. 2012.

[6] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," J. Cryptology, vol. 13, no. 3, pp. 361–396, 2000.