IJRRECS/August 2015/Volume-3/Issue-8/4560-4564 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN INNOVATIVE PROPOSAL TOWARDS FLEXIBLE SHARING OF CLOUD DATA

Anand Kumar Sharma[1], G.Jacob Jaya Raj[2]

[1]M.Tech Student, Dept of CSE, S.V College of Engineering & Technology, Moinabad, R.R Dist, T.S, India

[2]Associate Professor, Dept of CSE, S.V College of Engineering & Technology, Moinabad, R.R Dist, T.S, India

ABSTRACT:

Expansion for data outsourcing is used as an important knowledge for several applications. In the recent times, the efforts that were made earlier mainly spotlight on minimization of communication needs. In the recent cryptography techniques, the basic problem is regarding leveraging of confidentiality of data to carry out cryptographic functions numerous times. We make a study on making of decryption key more commanding so that it permits decryption of numerous cipher-texts, devoid of its size increase. We commence an outstanding public-key encryption known as key-aggregate cryptosystem. Cryptographic methods of key assignment decreases spending in storing as well as managing of secret keys for wide-ranging cryptographic use. We learn a novel cryptosystems of public-key that produce constant size cipher-texts for competent delegation of decryption rights for possible cipher-texts. Our method is flexible when compared to hierarchical key assignment that saves spaces when the entire key-holders distribute a related set of privileges.

Keywords: Data outsourcing, Key-aggregate cryptosystem, Cryptography techniques, Decryption key, Cipher-texts, Hierarchical key assignment.

1. INTRODUCTION:

In enterprise scenery, there is an enhancement for data outsourcing that motivates in considered managing of corporate information. Users by means of modern wireless expertise access to most of their files by mobile phone in several areas of world. Identification of an effective means to allocate partial information in cloud storage is not trivial [1]. In cloud storage environment sharing of data is important functionality. When dataprivacy is considered, the traditional way for making sure is to depend on server to impose access control subsequent to authentication will expose data. Users of cloud will not imagine that cloud server will do a good job regarding confidentiality. In our work we study on making of the decryption key more commanding so that it permits decryption of numerous cipher-texts, devoid of its size increase. In our work efficiently as well as flexible sharing of data with others in cloud storage was considered. Our approach is additionally flexible when compared to hierarchical key assignment that saves spaces when the entire key-holders distribute a related set of privileges. We introduce an exceptional public-key encryption known as key-aggregate cryptosystem.

2. METHODOLOGY:

In cloud storage environment sharing of data is important functionality. We study on making of the decryption key more commanding so that it permits decryption of numerous cipher-texts, devoid of its size increase. We study novel cryptosystems of public-key that generate constant size cipher-texts for competent delegation of decryption rights for possible cipher-texts. Secret key holder release a continuous size aggregate key for cipher-text set in cloud storage, however encrypted files exterior to set remain private [2][3]. One can combine secret keys and build them as single key, however encompassing all keys that are being aggregated. Compact aggregate key is sent towards others by means of extremely restricted secure storage. We study on making of decryption key more commanding so that it permits decryption of numerous cipher-texts, devoid of its size increase. For scheming of an effective public-key encryption system supporting effective delegation so that cipher-texts is decryptable by means of a continuous size decryption key. We solve it by means of

introduction of an exceptional public-key encryption known as key-aggregate cryptosystem in which users encrypts a message in public-key, and also in identifier of cipher-text known as class. Cipher-texts are considered as various classes and the owner of key r holds a master-secret key that extracts secret keys for a variety of classes. Extracted key might be an aggregate key for single class, but merge authority of several such keys. Key-aggregate method of encryption consists of five algorithms. The data owner confirms the parameter of public system by means of Setup and produces a secret key pair by means of KeyGen. Messages are encrypted by means of usage of Encrypt who makes a decision of the ciphertext class that is connected with the encrypted plaintext message. Owner of the data makes usage of master-secret to produce aggregate decryption key intended for a set of cipher text classes by the use of Extract. The keys that are generated are passed to delegates effectively. Any user by means of an aggregate key will decrypt the cipher-text that is provided that class of cipher-text is contained within aggregate key by means of Decrypt. The property of key aggregation is particularly helpful when we imagine delegation to be well-organized as well as flexible.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Cryptographic methods of key assignment aim to reduce expenditure in storing as well as managing of secret keys for wide-ranging cryptographic use. Usage of a tree structure, a key for a specified branch will be used to obtain the keys of its descendant nodes. For the most of the methods construct keys in support of symmetric-key cryptosystems, although key derivations might necessitate modular arithmetic which are usually pricier than symmetric-key operations [4]. Hierarchical methods can resolve the difficulty partly when one aims to distribute all files in a convinced branch within hierarchy. Number of keys enhances with number of branches and it is not likely to occur by a hierarchy that save number of entire keys to be approved for the entire individuals. Identity based encryption is a type of public-key encryption where public-key of user is set as identity string of user. There is a trustworthy party known as private key generator in Identity based encryption that holds a master-secret key and provide a secret key towards each user

regarding user identity. The encryptor takes public parameter as well as a user identity for encrypting of a message. The recipient decrypts cipher text by means of secret key. Attribute-based encryption permits each of the cipher-text that is to be connected by an attribute, as well as master-secret key holder can extract a secret key for a policy of attributes with the intention that a cipher-text is decrypted by means of key when its connected attribute conforms to policy. The most important issue within attribute based encryption is collusion resistance but not compactness of secret keys. Certainly size of key regularly enhances linearly with number of attributes it includes, or else cipher text-size is not stable. We study novel cryptosystems of public-key that generate constant size cipher-texts for competent delegation of decryption rights for possible cipher-texts. Any set of secret keys make them as single key, however encompassing all keys that are being aggregated and compact aggregate key is sent towards others by means of extremely restricted secure storage. Secret key holder release an unbroken size aggregate key for cipher-text set in cloud storage, however encrypted files exterior to set remain private. We set up an exceptional public-key encryption known as key-aggregate cryptosystem. Designing of our fundamental system is inspired from collusion-resistant broadcast encryption method that is projected by Boneh et al. Even though their scheme manages stable size secret keys, each key has power for decryption of cipher-texts that are connected towards a particular index. While novel public-key is basically treated as a novel user, one might have concern that key aggregation all across two autonomous users is not feasible [5]. We attain local aggregation that means secret keys in same branch can constantly be aggregated. Our benefit is still conserved when compared to quaternary trees within hierarchical approach, where latter moreover delegate's decryption power for the entire number of keys will be similar as number of classes. Our approach is additionally flexible when compared to hierarchical key assignment that saves spaces when the entire key-holders distribute a related set of privileges [6].

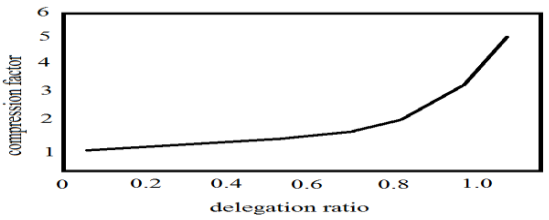

Fig1: an overview of Compression achieved by tree-based approach.

4. CONCLUSION:

More superior cryptographic methods of key assignment maintain access policies that are formed by means of an acyclic graph or else a cyclic graph. In our work we study about decryption key which is more commanding so that it permits decryption of numerous cipher-texts, devoid of its size increase. An exceptional public-key encryption known as key-aggregate cryptosystem was introduced and flexible sharing of data with others in cloud storage was considered. We make a study of novel cryptosystems of public-key that generate constant size cipher-texts for competent delegation of decryption rights for possible cipher-texts. For consideration of public-key encryption system that supports effectual delegation so that ciphertexts is decryptable by means of a continuous size decryption key. We solve it by means of introduction of an exceptional public-key encryption known as key-aggregate cryptosystem. Our approach is efficient when compared to hierarchical key assignment that saves spaces when the entire key-holders distribute a related set of privileges. Designing of our system is motivated from collusion-resistant broadcast encryption method.

REFERENCES

[1] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.

[2] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.

[4] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Trans. Knowledge and Data Eng., vol. 14, no. 1, pp. 182-188, Jan./Feb. 2002.

[5] G. Ateniese, A.D. Santis, A.L. Ferrara, and B. Masucci, "Provably- Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryptology, vol. 25, no. 2, pp. 243-270, 2012.

[6] R.S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95-98, 1988.