IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENHANCED SECRET SHARING PROTOCOL TO INCREASE FORWARD AND BACKWARD SECURITY FOR CLOUD IN BIGDATA

[1]Jayashee L., [2]Ms. Anita Madona M.,

[1]Research Scholar, [2]Assistant Professor

[1]Computer Science,

[1]Auxilium College (Autonomous), Gandhinagar, Vellore -6, Tamilnadu, India.

Abstract: A cloud-based big data sharing system utilizes a storage facility from a cloud service provider to share data with legitimate users. In traditional solutions, cloud provider stores the shared data in the huge data point outside the trusted authority of the data owner, which may produce insecurity for information confidentiality. In order to overcome this Enhanced Secret Sharing Cluster Key management (ESSCK) protocol is proposed. For this purpose first, an Enhanced Secret Sharing scheme is used to construct faster encryption and decryption process. Second, a Logical Key Hierarchy (LKH) is used to process a simple and effective key numbering method. By using this technique the new user and the previous user cannot predict the new key from the cloud. To meet the protocol forward security and backward security the Logical Key Hierarchy (LKH) method is proposed.

Simulation results using CloudSim tool is used to shows that, LKH has improved security and the protocol ESSCK could significantly reduce the computation cost of cluster user in the rekeying process.

Index Terms - Big data, cloud provider, secret sharing, Logical Key Hierarchy, Forward security, Backward security.

I. INTRODUCTION

Big data means storing large amount of data, in which the data can be “structured, semi-structured and unstructured data” collected from the different sources at rapid speed. The big data scanning helps the institution to stay active, work faster, it is a profitable, and also deliver percipient to find and increase in efficiency. But the usual storage devices are not comfortable in support of the big data because of its less memory space. To have an improved different storing and processing of big data, the Cloud Computing was developed.

Cloud Computing is a new enumerating model, in whole all the resources are stored in a form of cloud through Internet. The cloud resources can be exploited to many operations and services dynamically. Cloud computing also entrust remote services with a user's data, software and calculation. Cloud computing consists of hardware and software resources and made obtainable on the Internet, which is managed by the third-party services. Cloud computing also supports for scalability, so it is possible to store huge amount of data in the cloud.

While using big data in cloud, Cloud security is an important issue when storing and accessing the information in cloud. So, the security requirements must dramatically increase while accumulate the individual data on cloud environment.

Build precautions device for cloud storage space is not an easy task. Because the collective information on the cloud is not in be in a command of genuine participants, and the cluster records should be working on the command of the legal user. And there must be protective steps to be taken for information privacy, honesty, verification and safety.

II Literature Review

Cloud Computing are vulnerable against security attacks. While, rising amount of party, devices and application inside the cloud, it leads to the unpredictable expansion of records in authorization point, which makes it extra complicated to have proper access control . The shared data on the cloud can be adapted by the cloud supplier or by system attackers, resulting in loss of data. Defending the collective data from illegal deletion, alteration and production is a complicated task. There is a difficulty of forward and backward protection during the cluster key management which need a little adding just before the protocol, to have a well-organized dynamic method of cluster client. The significant challenge is to create the safe and well-organized algorithm for security in cloud.

Disadvantage

- There is a problem of forward and backward security in the group key management.
- Only static members are used in the group for sharing the data.

III Working of ESSCK Protocol Model

To enable the benefits of the big data technologies, security and privacy issues is addressed first and then the support security services cluster key management techniques is used. This deals with a solution for the forward and backward security for cloud computing in big data.

Proposed method uses an Enhanced Secret Sharing Cluster Key management (ESSCK) protocol. Where, two separate methods are used for securing the data in sharing system. First method used is secure cluster key management technique to defend the pooled data with the key and carry out the encryption and decryption process. Second method clusters key to generally manage the independent third party. Right of entry to be in charge of make the information to be access only by the genuine user.

To address the forward and backward security problem while sharing the data, a simple and efficient Logical Key Hierarchy technique is used. Here, as soon as a associate join in the cluster otherwise leaves the cluster the cluster key must be changed. As soon as a associate joins a cluster, the novel client cannot acquire the preceding cluster key, which is called as backward security. On the previous hand when a client leaves a cluster he can economically compute the novel key, once a leaving client cannot acquire a cluster key is called as forward security. Not only satisfy the security restriction, it also minimizes the computation charge along with storage price of the rekeying process.

Advantage

- Dynamic group members are used in the group key management technique.
- Here the forward security and backward security was obtained.
- Rekeying process is used to generate the new key.

IV Conclusion

To solve the problem of forward as well as backward security during the key sharing method based on the LKH method, An Enhanced Secret Sharing Cluster Key Management Protocol based on a new secret-sharing scheme proposed. Firstly, by designing a new secret sharing scheme, it is an efficient encryption and decryption algorithm . The ESSCK scheme is also extra resourceful on the cluster-client side. On the basis of ensure protection, the effectiveness of decrypting rekeying messages by cluster clients is enhanced. According to the testing results, the future protocol can extensively decrease the estimate cost of cluster clients in the rekeying method.

Future Work

In future, Enhanced One way Functional Tree (EOFT) can be used for better performance than the LKH algorithm. In EOFT a unique secret key is shared to the new client. EOFT will not modify all the keys in the cluster which the client knows, whereas the LKH changes all the keys in the cluster, when a client joins or leaves a cluster. Since the EOFT will not use the keys to encrypt any message, it will not alter the keys supplied to the cluster clients. So for better Key generation and Key distribution process EOFT can be used for the future work.

REFERENCES

[1]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacypreserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362_375, Feb. 2013.

[2]. S. Tanada, H. Suzuki, K. Naito, and A. Watanable, ``Proposal for secure group communication using encryption technology," in *Proc. 9th Int. Conf.Mobile Comput. Ubiquitous Netw.*, Oct. 2016, pp. 1_6.

[3]. J. Zhou *et al.*, ``Securing outsourced data in the multi-authority cloud with _ne-grained access control and ef_cient attribute revocation," *Comput. J.*,vol. 60, no. 8, pp. 1210_1222, Aug. 2017.

[4]. R. Ahuja, S. K. Mohanty, and K. Sakurai, ``A scalable attribute-set-based access control with both sharing and full-_edged delegation of access privileges in cloud computing," *Comput. Elect. Eng.*, vol. 57, pp. 241_256, Jan. 2017.

[5]. J. Thakur and N. Kumar, ``AES and blow_sh: Symmetric key cryptography algorithms simulation based performance analysis," *Int. J. Emerg. Technol.Adv. Eng.*, vol. 1, no. 2, pp. 6_12, Dec. 2011.

[6]. E. Fujisaki, T. Okamoto, ``Secure integration of asymmetric and symmetric encryption schemes," *J. Cryptol.*, vol. 26, no. 1, pp. 80_101, Jan. 2013.

[7]. Y. S. Rao, ``A secure and ef_cient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Gener. Comput. Syst.*, vol. 67, pp. 133_151 Feb. 2017.

[8]. S. Jin-Shu, C. Dan, W. Xiao-Feng, and S. Yi-Pin, ``Attributed-based encryption schemes," *J. Softw.*, vol. 22, no. 6, pp. 1299_1315, 2011.

[9]. H. liu, Y. huang, and J. K. Liu, ``Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption," *Future Gener. Comput. Syst.*, vol. 52, pp. 67_76, Nov. 2015.

[10]. K. Huang *et al.*, ``PKE-AET: Public key encryption with authorized equality test," *Comput. J.*, vol. 58, no. 10, pp. 2686_2697, Oct. 2015.

[11]. L.Wu, Y. Zhang, K.-K. R. Choo, and D. He, ``Ef_cient and secure identitybased encryption scheme with equality test in cloud computing," *Future Gener. Comput. Syst.*, vol. 73, pp. 22_31, Aug. 2017.

[12]. K. Huang *et al.*, "PKE-AET: Public key encryption with authorized equality test," *Comput. J.*, vol. 58, no. 10, pp. 2686_2697, Oct. 2015.

[13]. L.Wu, Y. Zhang, K.-K. R. Choo, and D. He, "Efficient and secure identity based encryption scheme with equality test in cloud computing," *Future Gener. Comput. Syst.*, vol. 73, pp. 22_31, Aug. 2017.

[14]. P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin, "On minimizing energy cost in internet-scale systems with dynamic data," *IEEE Access*, vol. 5, pp. 20068_20082, 2017.

[15]. D.Wu, G. Zhang, and J. Lu, "A fuzzy preference tree-based recommender system for personalized business-to-business E-services," *IEEE Trans.Fuzzy Syst.*, vol. 23, no. 1, pp. 29_43, Feb. 2015.

[16]. X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, pp. 97_107, Jan. 2014.

[17]. X. Shi, L. X. Li, L. Yang, Z. Li, and J. Y. Choi, "Information _ow in reverse logistics: An industrial information integration study," *Inf. Technol.Manage.*, vol. 13, no. 4, pp. 217_232, Dec. 2012.

[18]. N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of Things: A survey," *IEEE Access*, vol. 4, pp. 5591_5606, May 2016.

[19]. "A Light weight Secure Data Sharing Scheme for Mobile Cloud computing". Ruixuan Li, Chenglin Shen, Heng He, Zhiyong Xu, Cheng-Zhong Xu 2014 in IEEE Transactions on Cloud Computing

[20]. "Security Techniques for Data Protection in Cloud Computing" Kire Jakimoski 2016 International Journal of Grid and Distributed Computing.