Result Analysis of Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Pinky Mehra
M.Tech Scholar
Department of Cyber Security,
Kailash Narayan Patidar
College of Science and
Technology, Bhopal, India

Vimal Shukla
Head of department
Department of Cyber Security,
Kailash Narayan Patidar
College of Science and
Technology, Bhopal, India

Tariq Siddiqui
Asst. Professor
Department of Cyber Security,
Kailash Narayan Patidar
College of Science and
Technology, Bhopal, India

ABSTRACT
The Benefited from Cloud Computing, clients can do a flourishing and moderate methodology for data sharing among gathering individuals within the cloud with the characters of low maintenance and small administration price. , we should always offer security guarantees for the sharing data files since they're outsourced. Unfortunately, due to the frequent modification of the attachment, allocation data whereas as long as privacy-preserving is still a difficult issue, especially for an untrusted cloud owed to the collusion hit. Moreover, for existing schemes, the security of key distribution depends on the secure line, however, to have such channel could be a strong assumption and is tough for practice. Finally, our theme can succeed fine efficiency, which implies that previous users needn't to update their personal keys for matters either a replacement user joins within the group or a user is revoked from the group.

Keywords
Access power, Privacy-preserving, Key distribution, Cloud compute

1. INTRODUCTION
Cloud computing, with the characteristics of natural data sharing and low support, offers a superior usage of resources. In Cloud Computing, cloud administration suppliers provide a reflection of boundless storeroom for customers to host data [1]. It offers customers some support with reducing their money related overhead of data administrations by moving the near administrations framework into cloud servers. However, security issues become the principle control as we tend to currently source the capacity of data that is probably delicate, to cloud suppliers. To safeguard data security, a typical methodology is to encode data records before the customers transfer the scrambled data into the cloud [2]. Unfortunately, it's hard to outline a protected and productive data sharing arrange, significantly for part groups within the cloud. Cloud computing, with the uniqueness of important information sharing and low support, offers AN improved misuse of assets. In cloud process, cloud administration suppliers provide a concept of unending room for customers to host information [1]. It will help customers to diminish their financial straightforwardness of information administrations by exchanging the neighborhood administration's framework into cloud servers. Then again, security worry turns into the basic disadvantage as we tend to now source the capability of information that is probably agreeable, to cloud suppliers. to require care of information privacy, a general move towards is to encrypt data documents before the customers transfer the encrypted data into the cloud [2]. Unfortunately, it's hard to outline a secure and effective information sharing arrange, significantly for dynamic groups within the cloud.

Cloud Computing, the long-held dream of computing as a utility, has the potential to transform an oversized a part of the IT business, creating software system even additional attractive as a service and shaping the method IT hardware is designed and purchased. Developers with innovative ideas for new internet services not need the big capital outlays in hardware to deploy their service or the human expense to work it. they have not be concerned about over provisioning for a service whose quality doesn't meet their predictions, therefore wasting costly resources, or under provisioning for one that becomes wildly popular, therefore missing potential customers and revenue. Moreover, companies with large batch-oriented tasks will get results as quickly as their programs will scale, since using a thousand servers for one hour prices no quite using one server for a thousand hours. This elasticity of resources, while not paying a premium for big scale, is new within the history of IT. Cloud Computing refers to each the applications delivered as services over the web and also the hardware and systems software within the datacenters that give those services. The services themselves have long been named as software system as a Service (SaaS). The datacenter hardware and software system is what we'll decision a Cloud. once a Cloud is formed offered during a pay-as-you-go manner to the general public, we tend to decision it a Public Cloud; the service being sold is Utility Computing. We tend to use the term personal Cloud to refer to internal datacenters of a business or different organization, not created offered to the general public. Thus, Cloud Computing is that the add of SaaS and Utility Computing, however doesn't include personal Clouds. People may be users or providers of SaaS, or users or providers of Utility Computing.

2. THEORY
2.1 System Model
A cloud computing design by combining with an example that a company uses a cloud to enable its staffs within the same group or department to share files. The system model consists of 3 totally different entities: the cloud, a group manager (i.e., the company manager), and an oversized variety of group members (i.e., the staffs) as illustrated in Fig.1. Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud isn't totally sure by users since the CSPs are very possible to be outside of the cloud users' sure domain. Like we tend to assume that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user information because of the protection of information auditing schemes, but can attempt to

learn the content of the stored information and also the identities of cloud users.

Fig. 1: System model

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the important identity of a dispute information owner. Within the given example, the group manager is acted by the administrator of the company. Therefore, we tend to assume that the group manager is absolutely sure by the opposite parties. Group members are a group of registered users that may store their private information into the cloud server and share them with others within the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically modified, because of the staff resignation and new employee participation within the company.

3. METHOD

A secure data sharing theme proposes, which may achieve secure key distribution and data sharing for dynamic group. the most contributions of this scheme include:

1. This provides a secure method for key distribution without any secure communication channels. The users will securely get their private keys from group manager with none Certificate Authorities because of the verification for the general public key of the user.
2. This scheme can do fine-grained access control, with the help of the group user list, any user within the group will use the source within the cloud and revoked users cannot access the cloud again when they're revoked.
3. This secure data sharing scheme which may be protected from collusion attack. The revoked users cannot be able to get the original data files, once they're revoked even if they conspire with the untrusted cloud. This scheme can do secure user revocation with the help of polynomial perform.
4. This scheme is able to support dynamic teams with efficiency, once a new user joins within the group or a user is revoked from the group, the personal keys of the opposite users don't need to be recomputed and updated.
5. This scheme provides a security analysis to prove the security of our scheme. Additionally, it conjointly performs simulations to demonstrate the efficiency of our scheme.

We can get some benefits from this scheme, they are:

1. This scheme achieves a secure key distribution and data sharing for dynamic group.
2. During this scheme the users will securely get their personal keys from group manager without any Certificate Authorities.
3. This scheme is protected from collusion attack.
4. This scheme is able to support dynamic groups with efficiency.

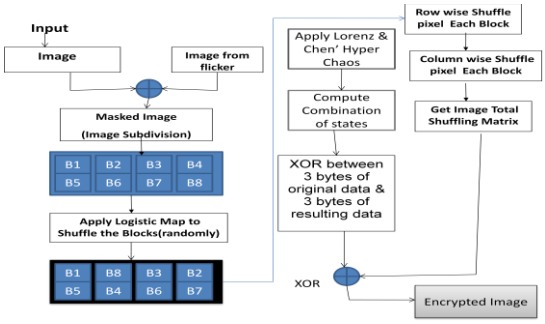

Fig. 2: Flow diagram of Encryption Algorithm

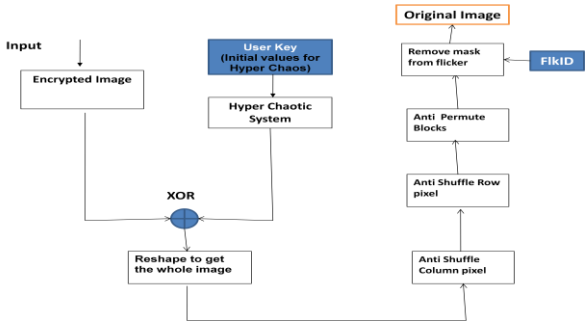

Fig.3: Flow diagram of Decryption Algorithm

4. RESULT

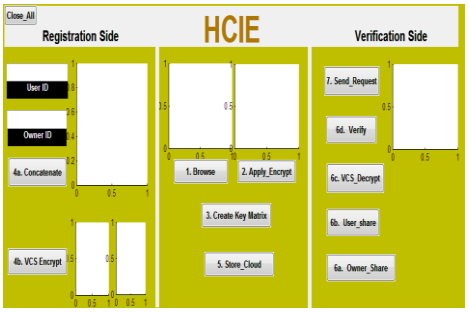

Fig.4 HCIF window

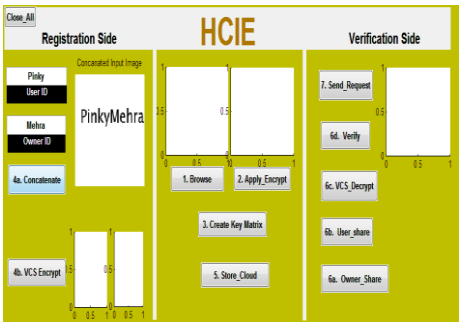

Fig.5 Show the concanated input image

Fig.6 Send Request Window

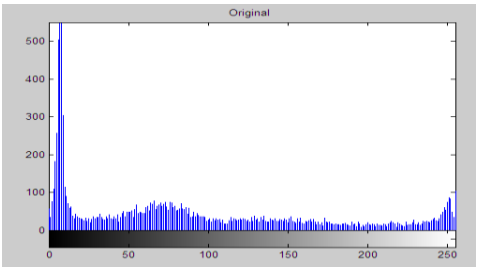

Fig.7 Original Data

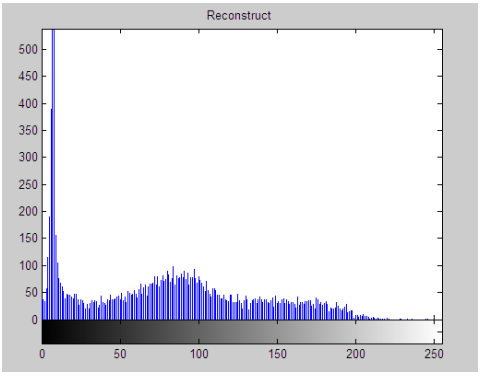

Fig.8 Reconstructed Data

5. CONCLUSION

This scheme designs a secure anti-collusion information sharing scheme for dynamic groups within the cloud. During this scheme, the users will securely obtain their private keys from group manager without any Certificate Authorities and secure communication channels. Also, this scheme is ready to support dynamic groups with efficiency, once a new user joins within the group or a user is revoked from the group, the private keys of the other users ought not to be recomputed and updated. Moreover, this scheme can do secure user revocation; the revoked users cannot be able to get the original information files once they're revoked even if they conspire with the untrusted cloud.

6. REFERENCES

[1] Zhongma Zhu, Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud" 10.1109/TPDS.2015.2388446, IEEE Transactions on Parallel and Distributed Systems

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[7] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[8] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content

sharing in public clouds," *IEEE Trans. on Know. and Data Eng.*, vol. 25, no. 11, pp. 2602-2614, 2013.

[10] Dolev, D., Yao A. C., "On the security of public key protocols", *IEEE trans. On Information Theory,* vol. IT-29, no. 2, pp. 198–208, 1983

[11] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[12] D. Boneh, X. Boyen, H. shacham, "Short group signature," *Proc. Int'*Cryptology Conf. Advances in Cryptology, pp.41-55, 2004.

[13] B. den Boer, Diffie–Hellman is as strong as discrete log for certain primes in Advances in Cryptology – CRYPTO 88, Lecture Notes in Computer Science 403, Springer, p. 530, 1988.

[14] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Proc. Int'l Conf.* Financial Cryptography and Data Security (FC), pp.136- 149, Jan. 2010.

[15] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.