ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Identity Based Integrity Checking and Attribute Based Data Sharing With Time Constraints Mechanism in Cloud Computing

[1] Apeksha Amol Unhale, [2] Nivedita Kadam
[1][2] Department of Computer Engineering, G. H. Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra

***Abstract* – Cloud computing is one among evolving technology today, giving versatile services. However, secure knowledge sharing is vulnerable in cloud computing environment. Full lifecycle privacy security is not enforced in Cloud; access management is difficult task to share sensitive knowledge on cloud servers. One among novel approach for secure knowledge self-destructing scheme is key Policy Attribute primarily based encoding with Time specified attributes i.e. (KP-TSABE). The cipher text is tagged with time interval and private key is associated with particular time instant.KP-TSABE supports user outlined authorization amount by providing fine-grained access control throughout the period. Once User specified expiration, time the info are securely, self-destructed.KP-TSABE scheme is secure beneath the choice l-bilinear Diffie-Hellman inversion assumption.**

Keywords: Sensitive Data, Secure Self-Destructing, Fine Grained Access Control, Privacy-Preserving, Cloud Computing

I. INTRODUCTION

With the speedy development of versatile cloud offerings, it becomes Associate in nursing increasing variety of liable to use cloud services to proportion facts during a crony circle within the cloud computing surroundings. Because of its not viable to place in effect complete life-cycle privacy security, get admission to manage becomes a tough endeavor, especially after we share sensitive info on cloud servers. The shared information in cloud servers, however, sometimes contains user's sensitive info and desires to be protected. Because the possession of the info is separated from the administration of them, the cloud servers could migrate user's information to alternative cloud servers in outsourcing or share them in cloud looking out. Therefore, it becomes an enormous challenge to shield the privacy of this shared information in cloud, particularly in cross-cloud and large information surroundings. To fulfill this challenge, it is necessary to style a comprehensive resolution to support user-defined authorization amount and to produce fine-grained access management throughout this era. The shared information to be self-destroyed once the user outlined expiration time.

II. LITERATURE SURVEY

1. "Privacy preserving public Auditing for shared data in the cloud," B. Wang,B. Li, and H. Li 2014:
In This paper, the identity of the signer on every block in shared knowledge is unbroken personal from public verifiers, efficiency verify shared knowledge integrity while not retrieving the whole file. Additionally it is ready to perform multiple auditing tasks at the same time rather than corroborative them one by one. The disadvantage is Ring signatures is utilize to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it is not able to distinguish who is the signer on each block. The problem with this system is 1.Traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations and how to prove data freshness. Batch Auditing can be used to distinguish who is the signer on each block 2.designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability. TPA can be implemented which will be able to support batch auditing.

2."Ensuring privacy and data freshness for public auditing of Shared data in cloud," Tina Esther Trueman ,P.Narayan asamy 2012:
It uses a novel methodology for making certain privacy and data freshness of shared knowledge in cloud exploitation Homomorphic authenticable ring signature (HARS) theme to preserve the user privacy and Overlay tree rule is employed for making certain that users the information with needed level of freshness. In addition, Third Party Auditor (TPA) audits the information keep within the cloud. He should be able to verify the trustiness of the CSP while not disclosing the identity of the users within the group. The disadvantage is malicious activities.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, March 2018

Made by the user cannot be detected. The problem with this system is to extend the traceability, which means only the original user, can reveal the identity of the signer in order to preserve the malicious activity made by the user in the group. Solution can be Batch Auditing can be used to distinguish who is the authorized person signer on each block.

3. "Toward Efficient and Privacy Preserving Computing in Big Data Era," Rongxing Lu, Hui Zhu, Ximeng Liu, Joseph K. Liu, and Jun Shao 2014:
Introduced an efficient and privacy-preserving cosine similarity(PCSC) computing protocol in response to the efficiency and privacy requirements of data mining in the big data era. 2. The proposed PCSC protocol is not only privacy preserving but also efficient. It is particularly suitable for big data analytics. The advantage is the computation overhead of the proposed PCSC protocol also increases when n is large. The disadvantage is Needs to provide unique privacy for some specific big data analytics. Introducing protocol like privacy computing to provide complete and unique security in big data era.

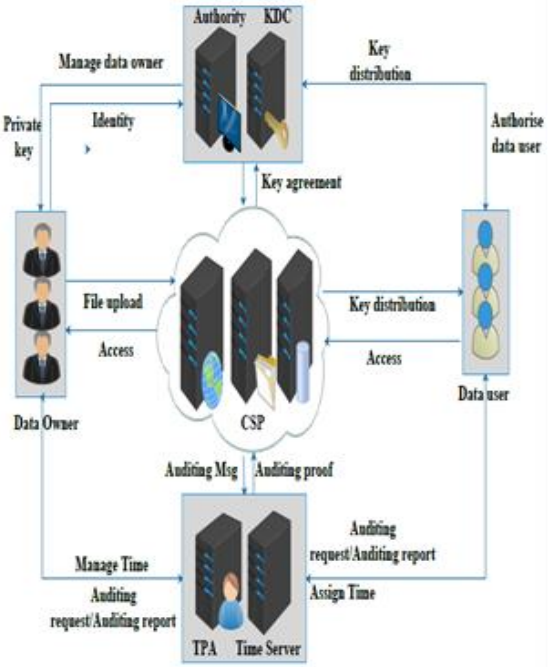
4. "Privacy-preserving access control model for big data cloud," S. Fugkeaw and H. Sato, International Computer Science and Engineering Conference (ICSEC), Chiang Mai, 2015, pp. 1-6.
Propose a novel access control model combining Role-based Access Control (RBAC) model, symmetric encryption, and cipher text attribute-based encryption (CP-ABE) to support fine-grained access control for big data outsourced in cloud storage systems. We also demonstrate the efficiency and performance of our proposed scheme through the implementation.

5. "Privacy-preserving public auditing for secure cloud storage," Wang, Cong, et al, IEEE Transactions on computers 62.2 (2013): 362-375.2013.
Propose a privacy-preserving public auditing system for data storage security in Cloud Computing. They made use of the Homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process. Which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the user's fear of their outsourced data leakage. Authors also claim that the proposed schemes are provably secure and highly efficient.

III. SYSTEM MODEL

In this paper, we discussed the different modules of the proposed system:

- Data Owner: Data owner can provide data or les that contain some sensitive information, which are used for sharing with his/her friends (data users). All these data, which is shared, are outsourced to the cloud servers to store these data.
- Authority: It is an indispensable entity, which is responsible for generating, distributing and managing all the private keys, and is trusted by all the other entities involved in the system.
- Time Server: It is a time reference server without any interaction with other entities involved in the system. It is responsible for a precise release time specification.
- Data Users: Data users are some peoples who passed the identity authentication and access to the data outsourced by the data owner. Notice that, the authorized users can only access the shared data during its authorization period.
- Cloud Servers: It contains almost unlimited storage space which is able to store and manage all the data or les in the system. Other entities with limited storage space can store their data.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, March 2018

- KDC: A typical operation with a KDC involves a request from a user to use some service. The KDC can use crypto logical techniques to demonstrate requesting users. It will additionally check whether or not Associate in every individual user has the correct to access the service, that is requested. If the authenticated user meets all prescribed conditions, the KDC can issue a ticket permitting access. The KDC generates secret keys for all the users according to their identities. The cloud user has large amount of files to be stored on cloud without keeping a local copy, and the cloud server has significant storage space and computation resources and provides data storage services for cloud users.
- TPA: TPA has expertise and capabilities that cloud users do not have and is trusted to check the integrity of the cloud data on behalf of the cloud user upon request. Each entity has their own obligations and benefits respectively. The cloud server could be self-interested, and for his own benefits, such as to maintain a good reputation, the cloud server might even decide to hide data corruption incidents to cloud users. The TPAs job is to perform the data integrity checking on behalf the cloud user, but the TPA is also curious in the sense that he is willing to learn some information of the user's data during the data integrity checking procedure.

IV. CONCLUSION

In this system, we investigated a new primitive known as identity-based remote data integrity checking for secure cloud storage. We formalized the security model of two important properties of this primitive; namely, attribute based mostly encryption and ideal data privacy. We tend to provide a new construction of this primitive and showed that it achieves hierarchical attribute based mostly encryption and ideal knowledge privacy. To reduce the overburden of knowledge owner because of user maximization, the time constraints mechanism are introduced. This mechanism will be able to manage the time for each user to access the cloud data as a result the cloud cost will be dramatically reduces. Both the numerical analysis and the implementation demon- stated that the proposed system is efficient and practical.

V. REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.

[2] Tina Esther Trueman ,P.Narayan asamy, "Ensuring privacy and data freshness for public auditing of Shared data in cloud," 2012.

[3] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," Network, IEEE, vol. 28, no. 4, pp. 46–50, 2014.

[4] Varsha Govindrao Kulkarni, Dr. Kishor Wagh, "Review on Privacy Preserving Deep Computation Model on Cloud for Big Data Feature Learning," Cloud Computing, 2015.

[5] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago.

[6] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," International Journal of Network Security, vol. 16, no. 4, pp. 351–357, 2014.

[7] Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005, ser. LNCS, vol. 7371. Springer, 2005, pp. 457–473.

[8] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and Communications Security. ACM, 2006, pp. 89–98.

[9] F. Chan and I. F. Blake, "Scalable, server-passive, useranonymous timed release cryptography," in Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504–513.

[10] K. G. Paterson and E. A. Quaglia, "Time-specific encryption," in Security and Cryptography for Networks. Springer, 2010, pp. 1–16.

[11] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, "Large universe decentralized key-policy attribute-based encryption," Security and Communication Networks,

2014. [Online]. Available: http:// dx. doi. org/ 10. 1002 /sec.997

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy. IEEE, 2007, pp. 321– 334.

[13] L. Cheung and C. C. Newport, "Provably secure ciphertext policy abe," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456– 465.

[14] Waters, "Ciphertext-policy attribute based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography–PKC 2011, pp. 53–70, 2011.

[15] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.