Data Security with Time Constraint in Clouds

M. S. Patel1[1] S. S. Londhe1[2] S. D. Mulik1[3] N. S. Shinde1[4]
[1,2,3,4]B.E. Students
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]SVPM's C.O.E. Malegaon (Bk.), 413115, Savitribai Phule, Pune University, Maharashtra, India

Abstract— Cloud computing is one of evolving technology nowadays, giving versatile services. But secure data sharing is susceptible in cloud computing environment. Full lifecycle privacy security is not implemented in Cloud, access control is challenging task to share sensitive data on cloud servers. One of novel approach for secure data self-destructing scheme is Key Policy Attribute Based Encryption with Time Specified attributes i.e. (KP-TSABE). The cipher text is labeled with time interval and private key is associated with particular time instant.KP-TSABE supports user defined authorization period by providing fine grained access control during the period. After User specified expiration time the data will be securely self-destructed.KP-TSABE scheme is secure under the decision 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 flexible cloud offerings, it becomes an increasing number of vulnerable to use cloud services to proportion facts in a chum circle in the cloud computing surroundings. Because it is not viable to put in force complete life-cycle privacy security, get admission to manage becomes a difficult undertaking, in particular when we share sensitive information on cloud servers.

The shared data in cloud servers, however, usually contains user's sensitive information and needs to be well protected. As the ownership of the data is separated from the administration of them, the cloud servers may migrate users data to other cloud servers in outsourcing or share them in cloud searching. Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, especially in cross cloud and big data environment. In order to meet this challenge, it is necessary to design a comprehensive solution to support user-defined authorization period and to provide fine grained access control during this period. The shared data should be self-destroyed after the user defined expiration time.

II. LITERATURE SURVEY

A. Attribute-based encryption:

Attribute-based encryption is one of the vital applications of fuzzy identification-primarily based encryption [7]. ABE comes in favours called KP-ABE [8][11] and cipher text policy ABE (CP-ABE) [12][13]. In CP-ABE, the cipher text is associated with the get entry to structure while the non-public key carries a set of attributes. Be then court docket et al. proposed the first CPABE scheme [12], the disadvantage in their scheme is that safety proof became handiest built under the well-known institution version. To deal with this weak point, Cheung et al. supplied any other construction beneath a trendy model [13]. Waters used a linear secret sharing scheme (LSSS) matrix as a preferred set of get entry to structures over the attributes and proposed an efficient and provably at ease CP-ABE scheme beneath the usual version [14]. In KP-ABE, the concept is reversed: the cipher textual content consists of a set of attributes and the personal secret is related to the get entry to structure. The first production of KP-ABE scheme was proposed in [8]. in their scheme, when a user made a secret request, the depended on authority determined which aggregate of attributes need to seem within the cipher textual content for the user to decrypt. rather than the use of the Shamir mystery key technique [15] inside the personal key, this scheme used a extra generalized shape of secret sharing to put into effect a monotonic get right of entry to tree. Ostrovsky et al. supplied the first KP-ABE machine which supports the no monotone formulas in key rules [16]. Yu et al. used a combining technique of KP-ABE, proxy encryption, and lazy re-encryption which permits the records proprietor to delegate most of the computation obligations concerned in fine-grained information access control to untrusted cloud servers without disclosing the underlying facts contents [17]. Tysowski et al. modified the ABE and leveraged re-encryption algorithm to endorse a novel scheme to guard mobile user's facts in cloud computing environment [18]. due to the shortage of time constraints, the above-stated ABE schemes do not guide user-defined authorization duration and comfy self-destruction after expiration for privacy-maintaining of the records lifecycle in cloud computing.

B. Secure self-destruction scheme:

A famous method for addressing this problem is relaxed deletion of touchy statistics after expiration while the facts became used [19]. currently, Cachin et al. hired a coverage graph to explain the relationship among attributes and the protection elegance and proposed a coverage-based secure statistics deletion scheme [20]. Reardon et al. leveraged the graph concept, Btree shape and key wrapping and proposed a unique approach to the design and analysis of at ease deletion for persistent storage devices [21]. due to the homes of bodily garage media, the above-cited methods aren't appropriate for the cloud computing environment as the deleted statistics may be recovered without difficulty within the cloud servers [22]. A records self-destructing scheme, first proposed by way of Geambasuetal.[23],is a promising method which designs a Vanish device enables customers to control over the lifecycle of the touchy facts. Wang et al. improved the Vanish device and proposed a relaxed self-destructing scheme for digital facts (SSDD) . in the SSDD scheme, a data is encrypted right into a ciphertext, that is then associated and extracted to make it incomplete to withstand towards the traditional cryptanalysis and the brute-pressure attack. Then, both the decryption key and the extracted ciphertext are allotted into a distributed hash desk (DHT) network to put

into effect self-destruction after the update length of the DHT network. however, Wolchok et al. made a number of experiments and confirmed that the Vanish machine is susceptible to Sybil attacks by the use of the Vuze DHT community. So the security of the SSDD scheme is likewise questionable. To cope with this hassle, Zeng et al.

C. Time Specific Encryption:

A famous method for addressing this problem is relaxed deletion of touchy statistics after expiration while the facts became used [19]. currently, Cachin et al. hired a coverage graph to explain the relationship among attributes and the protection elegance and proposed a coverage-based secure statistics deletion scheme [20]. Reardon et al. leveraged the graph concept, Btree shape and key wrapping and proposed a unique approach to the design and analysis of at ease deletion for persistent storage devices [21]. due to the homes of bodily garage media, the above-cited methods aren't appropriate for the cloud computing environment as the deleted statistics may be recovered without difficulty within the cloud servers [22]. A records self-destructing scheme, first proposed by way of Geambasuetal.[23],is a promising method which designs a Vanish device enables customers to control over the lifecycle of the touchy facts. Wang et al. improved the Vanish device and proposed a relaxed self-destructing scheme for digital facts (SSDD). in the SSDD scheme, a data is encrypted right into a ciphertext, that is then associated and extracted to make it incomplete to withstand towards the traditional cryptanalysis and the brute-pressure attack. Then, both the decryption key and the extracted ciphertext are allotted into a distributed hash desk (DHT) network to put into effect self-destruction after the update length of the DHT network. however, Wolchok et al. made a number of experiments and confirmed that the Vanish machine is susceptible to Sybil attacks by the use of the Vuze DHT community . So the security of the SSDD scheme is likewise questionable. To cope with this hassle, Zeng et al. proposed a SeDas gadget, which is a singular integration of cryptographic techniques with active storage techniques. Xiong et al. leveraged the DHT network and identity-based totally encryption (IBE) and proposed an IBE-based at ease self-destruction (ISS) scheme [22]. to be able to guard the confidentiality and privacy protection of the composite files inside the entire lifecycle in cloud computing, Xiong et al. carried out the ABE algorithm to recommend a cozy self-destruction scheme for composite documents (SelfDoc). these days, Xiong et al. employed identification-based totally timed-launch encryption (identification-TRE) algorithm [9] and the DHT network and proposed a full lifecycle privacy protection scheme for sensitive facts (FullPP), which is capable of offer full lifecycle privateness safety for customers' touchy records with the aid of making it unreadable earlier than a predefined time and robotically destructed after expiration [3]. the principle idea of the above-noted schemes is that they respectively integrate specific cryptographic techniques with the DHT network to offer finegrained information get admission to control during the lifecycle of the included records and to put into effect records selfdestruction after expiration. however, the usage of of the DHT network will result in the fact that the lifecycle

III. CONTRIBUTION

In this paper, we advise a KP-TSABE scheme, that is a novel comfy self-destructing scheme for records sharing in cloud computing. We first introduce the perception of KP-TSABE, formalize the model of KP-TSABE and give the security version of it. Then, we give a specific creation technique about the scheme. Eventually, we prove that the KP-TSABE scheme is secure. Specially, KP-TSABE has the following advantages with regard to protection and fine-grained get admission to manage in comparison to other comfortable self-destructing schemes.

1) KP-TSABE supports the characteristic of user defined authorization length and ensures that the touchy information cannot be read each earlier than its preferred release time and after its expiration.
2) KP-TSABE does now not require the proper assumption of "No attacks on VDO earlier than it expires".
3) KP-TSABE is capable of put into effect fine-grained get admission to control during the authorization duration and to make the touchy information self-destruction after expiration without any human intervention.
4) KP-TSABE is validated to be secure beneath the usual version by way of the usage of the l-bilinear DiffieHellman inversion assumption.

IV. SYSTEM MODEL

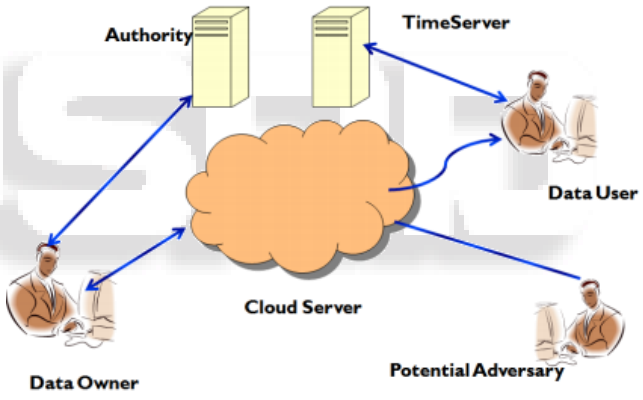

Fig. 1:

- Data Owner. Data owner can provide data or files that contain some sensitive information, which areusedforsharingwithhis/herfriends(datausers). All these shared data are outsourced to the cloud servers to store.
- 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 shared data can only be accessed by the authorized users during its authorization period.
- Cloud Servers. It contains almost unlimited storage space which is able to store and manage all the data or files in the system. Other entities with limited storage space can store their data to the cloud servers.

- Potential Adversary. It is a polynomial time adversary which have all access to Cloud Server.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditingfor shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.
[2] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.
[3] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, "A full lifecycle privacy protection scheme for sensitive data in cloud computing," Peerto-Peer Networking and Applications. [Online]. Available: http://dx.doi.org/10.1007/s12083-014-0295-x
[4] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 142–157, 2013.
[5] 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.
[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.
[16] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007, pp. 195–203.
[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th IEEE International Conference on Computer Communications. IEEE, 2010, pp. 1–9.
[18] P. Tysowski and M. Hasan, "Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 172–186, 2013.
[19] J. Reardon, D. Basin, and S. Capkun, "Sok: Secure data deletion," in Proceedings of the 34th IEEE Symposium on Security and Privacy. IEEE, 2013, pp. 1–15.
[20] Cachin, K. Haralambiev, H.-C. Hsiao, and A. Sorniotti, "Policy-based secure deletion," in Proceedings of the ACM Conference Computer and Communications Security. ACM, 2013, pp. 152–167.
[21] J. Reardon, H. Ritzdorf, D. Basin, and S. Capkun, "Secure data deletion from persistent media," in Proceedings of the 2013 ACM Conference on Computer and Communications Security. ACM, 2013, pp. 271–284.
[22] J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, "A secure selfdestruction scheme with ibe for the internet content privacy," Chinese Journal of Computers, vol. 37, no. 1, pp. 139–150, 2014.
[23] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in Proceedings of the 18th USENIX Security Symposium, 2009, pp. 299–315.

