International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

Survey on Data Security with Time Constraint in Clouds

Prajakta Nikam[1], Payal Tapadiya[2], Sumedha Gaikwad[3], Priyanka Ambugle[4]

[1,2,3,4]*B.E. Students Department of Information Technology, Sinhgad Institute of Technology, Savitribai Phule, Pune University, Maharashtra, India*

Abstract— with the rapid development of versatile cloud services, it becomes increasingly susceptible to use cloud services to share data in a friend circle in the cloud-computing environment. Since it is not feasible to implement full lifecycle privacy security, access control becomes a challenging task, especially when we share sensitive data on cloud servers. In order to tackle this problem, we propose a key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a novel secure data self-destructing scheme in cloud computing. In the KP-TSABE scheme, every ciphertext was labeled with a time interval while private key is associated with a time instant. The ciphertext can only be decrypt if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. The KP-TSABE is able to solve some important security problems by supporting user defined authorization period and by providing fine-grained access control during the period. The sensitive data will be securely self-destructed after a user-specified expiration time. The KP-TSABE scheme is proved secure under the decision l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) assumption. Comprehensive comparisons of the security properties indicate that the KP-TSABE scheme proposed by us satisfies the security requirements and is superior to other existing schemes

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 increasing style of vulnerable to use cloud services to proportion facts throughout a brother circle among the cloud computing surroundings. As results of its not viable to position in result complete life-cycle privacy security, get admission to manage becomes a tricky endeavor, particularly once we have a tendency to share sensitive information on cloud servers.

The shared data in cloud servers, however, generally contains user's sensitive information and needs to be protected. Because of the possession of the information is separated from the administration of them, the cloud servers might migrate user's data to different cloud servers in outsourcing or share them in cloud looking. Therefore, it becomes a massive challenge to protect the privacy of this shared data in cloud, notably in cross-cloud and huge data surroundings. Therefore on fulfill this challenge; it is a necessity to vogue a comprehensive resolution to support user-defined authorization quantity and to supply fine-grained access management throughout this era. The shared data need to be self-destroyed once the user made public expiration time.

II. LITERATURE SURVEY

A. Attribute-based encryption:

Attribute-based Attribute-based encoding is one among the important applications of fuzzy identification-primarily primarily based encoding. ABE comes in favors known as KP-ABE and cipher text policy ABE (CP-ABE). In CP-ABE, the cipher text is related to the get entry to structure whereas the personal key carries a collection of attributes. Be then court docket et al. projected the primary CPABE theme, the disadvantage in their theme is that safety proof became handiest engineered underneath the well-known establishment version. To subsume this liability, Cheung et al. provided the other construction beneath a classy model. Waters used a linear secret sharing theme (LSSS) matrix as a most popular set of get entry to structures over the attributes associate degreed projected an economical and incontrovertibly comfortable CP-ABE theme to a lower place the standard version. In KP-ABE, the construct is reversed the cipher matter content consists of a collection of attributes and therefore the personal secret is expounded to the get entry to structure. The primary production of KP-ABE theme was projected. In their theme, once a user created a secret request, the relied on authority determined that mixture of attributes have to be compelled to appear inside the cipher matter content for the user to decode. instead of the employment of the Shamir mystery key technique within the private key, this theme used an additional generalized form of secret sharing to place into impact a monotonic get right of entry to tree. Ostrovsky et al. provided the primary KP-ABE machine that supports the no monotone formulas in key rules. Yu et al. used a combining technique of KP-ABE, proxy encoding, and lazy re-encryption, which allows the records owner to delegate most of the computation obligations involved in fine-grained data access management to untrusted cloud servers while not revealing the underlying facts contents. Tysowski et al. changed the ABE and leveraged re-encryption algorithmic rule to endorse a unique theme to protect mobile user's facts in cloud computing surroundings. Attributable to the shortage of your time constraints, the above-stated ABE

schemes don't guide user-defined authorization period and comfortable self-destruction when expiration for privacy-maintaining of the records lifecycle in cloud computing

B. Secure self-destruction scheme:

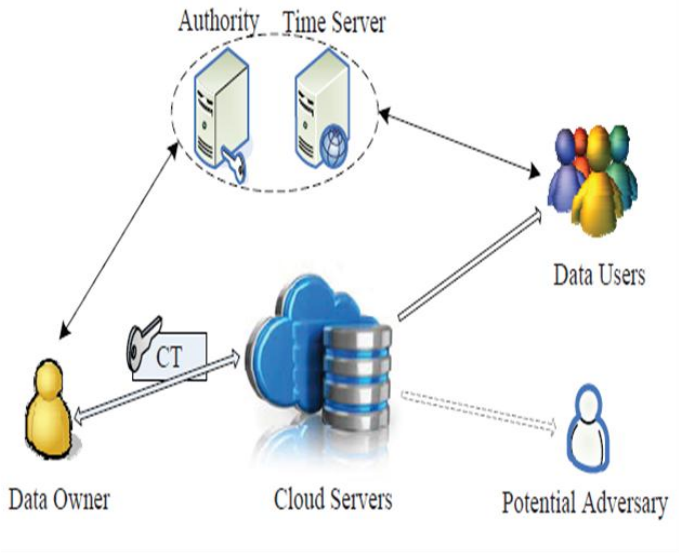
A noted technique for addressing this drawback is relaxed deletion of touchy statistics when expiration whereas the facts became used. Currently, Cachin et al. employed a coverage graph to elucidate the link among attributes and therefore the protection magnificence and projected a coverage-based secure statistics deletion theme. Reardon et al. leveraged the graph construct, Btree form and key wrapping and projected a novel approach to the planning and analysis of comfortable deletion for persistent storage devices. Attributable to the homes of bodily garage media, the above-cited strategies are not applicable for the cloud computing surroundings because the deleted statistics could also be recovered only inside the cloud servers. A records self-destructing theme, 1st projected by means of Geambasuetal, could be a promising technique that styles a Vanish device permits customers to regulate over the lifecycle of the touchy facts. Wang et al. improved the Vanish device and projected a relaxed self-destructing theme for digital facts (SSDD). Within the SSDD theme, information is encrypted right into a cipher text that has then associated and extracted to create it incomplete to face up to towards the standard cryptanalytics and therefore the brute-pressure attack. Then, each the decoding key and therefore the extracted cipher text area unit assigned into a distributed hash table (DHT) network to place Into impact self-destruction when the update length of the DHT network. However, Wolchok et al. created variety of experiments and confirmed that the Vanish machine is prone to Sybil attacks by the employment of the Vuze DHT community. Therefore, the security of the SSDD theme is likewise questionable. To deal with this problem, Zeng et al

C. Time Specific Encryption:

A noted technique for addressing this drawback is relaxed deletion of touchy statistics when expiration whereas the facts became used. Currently, Cachin et al. employed a coverage graph to elucidate the link among attributes and therefore the protection magnificence and projected a coverage-based secure statistics deletion theme. Reardon et al. leveraged the graph construct, Btree form and key wrapping and projected a novel approach to the planning and analysis of comfortable deletion for persistent storage devices. Attributable to the homes of bodily garage media, the above-cited strategies are not applicable for the cloud computing surroundings because the deleted statistics could also be recovered only inside the cloud servers. A records self-destructing theme, 1st projected by means of Geambasuetal, is a promising technique that styles a Vanish device permits customers to regulate over the lifecycle of the touchy facts. Wang et al. improved the Vanish device and projected a relaxed self-destructing theme for digital facts (SSDD). Within the SSDD theme, information is encrypted right into a cipher text that has then associated and extracted to create it incomplete to face up to towards the standard cryptanalytics and therefore the brute-pressure attack. Then, each the decoding key and therefore the extracted cipher text area unit assigned into a distributed hash table (DHT) network to place into impact self-destruction when the update length of the DHT network. However, Wolchok et al. created variety of experiments and confirmed that the Vanish machine is prone to Sybil attacks by the employment of the Vuze DHT community. Therefore, the security of the SSDD theme is likewise questionable. To deal with this problem, Zeng et al. projected a SeDas appliance that could be a singular integration of cryptographical techniques with active storage techniques. Xiong et al. leveraged the DHT network associate degreed identity-based altogether encoding (IBE) and projected an IBE-based comfortable self-destruction (ISS) theme. To be ready to guard the confidentiality and privacy protection of the composite files within the complete lifecycle in cloud computing, Xiong et al. applied the ABE algorithmic rule to suggest a comfy self-destruction theme for composite documents (SelfDoc). These days, Xiong et al. used identification-based altogether timed-launch encoding (identification-TRE) algorithmic rule [9] and therefore the DHT network and projected a full lifecycle privacy protection theme for sensitive facts (FullPP), that is capable of supply full lifecycle privateers safety for customers' touchy records with the help of creating it unclear previous a predefined time and robotically destructed when expiration [3]. The principle plan of the above-noted schemes is that they severally integrate specific cryptographical techniques with the DHT network to supply fine-grained data get admission to regulate throughout the lifecycle of the enclosed records and to place into impact records self-destruction when expiration. However, the usage of the DHT network can lead to the fact that the lifecycle.

III. SYSTEM DESCRIPTION

We propose a key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a novel secure data self-destructing scheme in cloud computing. In the KP-TSABE scheme, every ciphertext is labeled with a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. The KP-TSABE is able to solve some important security problems by supporting userdefined authorization period and by providing fine-grained access control during the period. The sensitive data will be securely self-destructed after a user-specified expiration time. The KP-TSABE scheme is proved secure under the decision l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) assumption. Comprehensive comparisons of the security properties indicate that the KP-TSABE scheme proposed by us satisfies the security requirements and is superior to other existing schemes.



Modules:

The system is proposed to have the following modules along with functional requirements.

Sensitive data, secure self-destructing fine-grained access control, privacy-preserving cloud computing

- Register

  In This Module New User Register The Information In The Order Of The List For Client Purpose.

- Login:

  In This Module User Can Login By Using His/Her Name And Key.

- Sensitive data:

  As the-state-of-the-art of the secure self-destruction scheme, both SSDD and FullPP have some limitations. First, SSDD does not consider the issue of the desired release time of the sensitive data the expiration time of both SSDD and FullPP schemes is limited by the DHT network and cannot be determined by the user. Second, SSDD and many other schemes are dependent on the ideal assumption of "No attacks on VDO (vanishing data object) before it expire". Third, it is demonstrated that the Vanish scheme is vulnerable to the Sybil attacks from the DHT network, the SSDD scheme and other schemes are similar. As a result, denoting that the encrypted data item can only be decrypted between The data owner encrypts his/her data to share with users in the system, in which every users key is associated with an access tree and each leaf node is associated with a time instant, The access tree of each user can be defined as a

- Secure self-destructing:

  A data self-destructing scheme, first proposed by Geambasu et al., is a promising approach which designs a Vanish system enables users to control over the lifecycle of the sensitive data. Wang et al. improved the Vanish system and proposed a secure self-destructing scheme for electronic data (SSDD). In the SSDD scheme, a data is encrypted into a ciphertext, self-destructing scheme for data sharing in cloud computing. We first introduce the notion of KP-TSABE, formalize the model of KP-TSABE and give the security model of it. Then, we give a specific construction method about the scheme. Finally, we prove that the KP-TSABE scheme is secure.

- Fine-grained access control

  In order to implement fine-grained access control, we associate every attribute in the attribute set with a time interval (authorization period). The attribute is valid if and only if the current time instant is in this time interval. Only if the valid attribute in the ciphertext satisfies the access tree in the key, the algorithm can decrypt the message correctly. The algorithm level of the KP-TSABE scheme includes four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

- Privacy-preserving:

  Due to the lack of time constraints, the above-mentioned ABE schemes do not support user-defined authorization period and secure self-destruction after expiration for privacy-preserving of the data lifecycle in cloud computing. Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment [5]. 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.

- Cloud computing

  Tysowski et al. modified the ABE and leveraged re-encryption algorithm to propose a novel scheme to protect mobile user's data in cloud computing environment. Due to the lack of time constraints, the above-mentioned ABE schemes do not support user-defined authorization period and secure self-destruction after expiration for privacy-preserving of the data lifecycle in cloud computing. It is a time interval from the creation of the shared data, authorization period to

expiration time. This paper provides full lifecycle privacy protection for shared data in cloud computing

- Upload:

  User Want To every File Upload Here This Module Convert to Your File Ciper Text Again Your Process Is Completed.

- Download:

  User Want to Download to Your File Here Its Before That Must Want To Key of the Data File Name And Key submitted Then Your Original File is Download.

VI. CONCLUSION

In cloud storage system, secure information destruction is one in all the problems that require to be addressed in information security.

Many information destruction schemes are projected in recent years. However, there are still some limitations. In this paper, we principally concentrate on the ciphertext destruction and propose a secure ciphertext self-destruction scheme with attribute-based encryption known as SCSD that applies the attribute-based encryption and the distributed hash table technology to the method of knowledge destruction within the cloud storage environment. Compared with the present schemes, our theme will resist the normal cryptanalysis attack as well because the Sybil attacks within the DHT network. Besides, the performance of SCSD scheme is comparatively effective and efficient.

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, "Cipher text - 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.