ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

An access control system with privilege separation based on privacy protection (PS-ACS)

[1] N.Akhil, [2] A.Jyothi
[1] M.Tech (CSE), [2] Asst Professor
[1][2] CVSR College

Abstract: With the rapid development of the computer technology, cloud-based services have become a hot topic. Cloud based services not only provide users with convenience, but also bring many security issues. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS).In the PS-ACS scheme, we divide the users into personal domain(PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement there ad access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature (IABS) which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

INTRODUCTION

Privacy In general privacy refers the condition or state of hiding the presence or view. There is a need to attain this state in the places where the confidential things are used such as data and files. In cloud data storage the privacy is need to attain for the data, user identity and on controls. Violation of privacy leads to major failure in the system. To maintain the data privacy, it is possible for a successful deployment and usage of any service.

Privacy issues in cloud Data in the cloud data storage has maintained at several distributed locations. CSP is the responsible person to maintain all the data securely. If proper security mechanism is implemented the security is violated at the storage service. Data can be accessed only by the person who is authorized. It is possible in this cloud model a CSP can read the client data for his purpose. Some competitor companies of data owner can give some amount to the CSP and get the access for the data. Internal workers in the CSP organization may access the data and give it to the business people for money. Government related data files like tender services, investigation documents, property checks may need by the industrialist. So the person contact the CSP and ask for the data. CSP can give it to the person on the basis of money or any other service. Identity of the famous person data like, Prime Minister, world famous sportsman, Actors personal data are accessed by the malicious persons to do such criminal activities. The access of a user is theft for performing some operation using their data. Some attackers are remove the data from the storage. Threats, malicious software are introduced to this storage for getting access and gain knowledge about the data. Privacy preservation Privacy deals with accessibility and availability of sensitive information to the intended recipients. Outsourced data accessed and modified only by the users who are having appropriate access privileges. Consider an organization have prepared and outsource their data in cloud. The outsourced data contents are given to the local administrator to place in cloud. It is recommended to ensure that the administrator cannot view or modify the data contents. After file outsourcing, no one including service provider can view or modify the contents. If service provider or local administrator is trying to read the file contents, it must not be done.
Privacy preservation deals with the kind of security in outsourced data. This could be ensured by using Cryptographic techniques.

EXISTING SYSTEM:

- Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed.

- In 2007, Bethen court et al. first proposed the ciphertext policy attribute-based encryption (CP-ABE).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

- Li et al presented data sharing scheme based on systemic attribute encryption, which endows different users' different access rights. But it is not efficient from the complexity and efficiency.

- Chen et al. proposed Key-Aggregate Encryption algorithm, effectively shortening the length of the ciphertext and the key, but only for the situation where the data owner knows the user's identity.

DISADVANTAGES OF EXISTING SYSTEM:

- The traditional access control strategy cannot effectively solve the security problems that exist in data sharing.
- This scheme does not consider the revocation of access permissions.
- It can easily cause key escrow issue.
- These existing schemes only focus on one aspect of the research, and do not have a strict uniform standards either.

PROPOSED SYSTEM:

- We propose a novel access control system called PSACS,which is privilege separation based on privacy protection.The system uses Key-Aggregate Encryption (KAE) schemeand Hierarchy Attribute-based Encryption (HABE) scheme toimplement read access control scheme in the PSD and PUDrespectively.

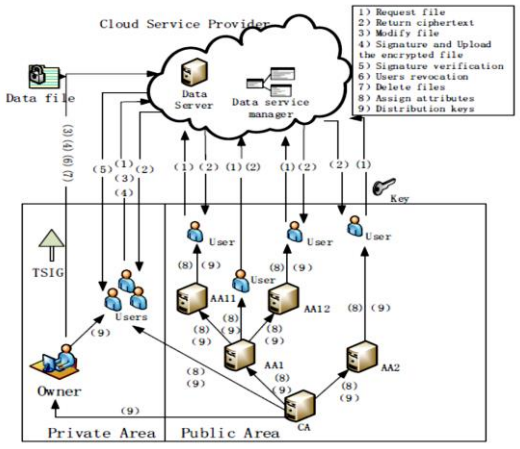
- The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data.

- Compared with the MAH-ABE scheme which does no trefer to the write access control, we exploit an Improved Attribute-based Signature (IABS)scheme to enforce write access control in the PSD. In this way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file.

ADVANTAGES OF PROPOSED SYSTEM:

- In this paper, we present a more systematic, flexible and efficient access control scheme.
- We provide a thorough analysis of security and complexity of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme.
- The evaluation results show the high efficiency of our scheme.

SYSTEM ARCHITECTURE:



CONCLUSION In this paper, we have proposed a privacy-preserving data publish-subscribe service for cloud-based platforms. Specifically, we have formulated the problem of data publishsubscribe system on cloud-based platforms by refining the security requirements. Then, we have proposed the PDPS scheme on top of the BP-ABE enabling the cloud server to do privacy-preserving bi-policy matching on the access policy defined by data publishers and the subscription policy defined by data subscribers. We have also demonstrated that the PDPS scheme is secure in standard model and efficient in practice. The PDPS scheme can be applied to achieve privacypreserving data publish-subscribe service on any cloud-based platforms. In our future work, we will

consider other matching patterns such as inequality matching, range matching and conjunctive matching etc.

REFERENCES

[1] A. Shikfa, M. ¨Onen, and R. Molva, "Privacy-preserving content-based publish/subscribe networks," in Emerging challenges for security, privacy and trust. Springer, 2009, pp. 270–282.

[2] S. Choi, G. Ghinita, and E. Bertino, "A privacy-enhancing content-based publish/subscribe system using scalar product preserving transformations," in Proceedings of the 21st International Conference on DatabaseandExpertSystemsApplications:PartI(DEXA'10) . Berlin,Heidelberg: Springer-Verlag, 2010, pp. 368–384.

[3] M. A. Tariq, B. Koldehofe, and K. Rothermel, "Securing broker-less publish/subscribe systems using identity-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 518–528, Feb. 2014.

[4] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., 2009.

[5] V. 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 (CCS'06). New York, NY, USA: ACM, 2006, pp. 89–98.

[6] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in Proceedings of the 3rd International Conference Palo Alto on Pairing-Based Cryptography (Pairing'09). Berlin, Heidelberg: Springer-Verlag, 2009, pp. 248–265.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P'07). Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography (PKC'11). Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[9] 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 Conference on Information Communications (INFOCOM'10). IEEE, 2010, pp. 534–542. [10] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIACCS'13). New York, NY, USA: ACM, 2013, pp. 523–528.

[11] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[12] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.

[13] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in Proceedings of the 20th USENIX Conference on Security (SEC'11). Berkeley, CA, USA: USENIX Association, 2011, pp. 34–34.

[14] M. Nabeel, S. Appel, E. Bertino, and A. Buchmann, "Privacy preserving context aware publish subscribe systems," in Network and System Security. Springer, 2013, pp. 465–478.

[15] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An efficient privacypreserving publish-subscribe service scheme for cloud computing," in GLOBECOM'10. IEEE, Dec 2010, pp. 1–5.

[16] C. Raiciu and D. S. Rosenblum, "Enabling confidentiality in contentbased publish/subscribe infrastructures," in Securecomm and Workshops, 2006. IEEE, 2006, pp. 1–11.

[17] M. Nabeel, N. Shang, and E. Bertino, "Efficient privacy preserving content based publish subscribe systems," in Proceedings of the 17th ACM Symposium on Access Control Models and Technologies

(SACMAT'12). New York, NY, USA: ACM, 2012, pp. 133–144.

[18] W. Rao, L. Chen, and S. Tarkoma, "Toward efficient filter privacy-aware content-based pub/sub systems," IEEE Trans. on Knowl. and Data Eng., vol. 25, no. 11, pp. 2644–2657, Nov. 2013.

[19] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proceedings of the 35th International Colloquium on Automata, Languages and Programming, Part II (ICALP'08). Berlin, Heidelberg: Springer-Verlag, 2008, pp. 579–591.

[20] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "An efficient and secure user revocation scheme in mobile social networks," in GLOBECOM'11. IEEE, 2011, pp. 1–5.

[21] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in Cloud Computing," Int. J. Secur. Netw., vol. 6, no. 2/3, pp. 67–76, Nov. 2011.

[22] X. Liang, M. Barua, R. Lu, X. Lin, and X. Shen, "Healthshare: Achieving secure and privacy-preserving health information sharing through health social networks," Computer Communications, vol. 35, no. 15, pp. 1910 – 1920, 2012.

[23] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[24] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11). New York, NY, USA: ACM, 2011, pp. 411–415.

[25] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," in TrustCom'11. IEEE, 2011, pp. 91–98.