IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10305

A Survey On Secure Data Group Sharing And Distribution With Multiowner Using Multicloud Storage Services

Mr. Dipak G. Hotkar[1], Prof. B.R.Solunke[2]

PG Student, Department of Computer Science & Engineering NBNSCOE, Solapur, India[1]

Assistant Professor, Department of Computer Science & Engineering, NBNSCOE, Solapur, India[2]

Abstract: With the fast development of cloud services, immense volume of knowledge is shared via cloud computing. Although cryptographic techniques are utilised to supply information confidentiality in cloud computing, current mechanisms cannot enforce privacy issues over ciphertext related to multiple house owners, which makes co-owners unable to fitly control whether or not information disseminators will truly air their information. during this paper, we have a tendency to propose a secure information cluster sharing and conditional dissemination theme with multi-owner in cloud computing, within which information owner will share personal information with a group of users via the cloud during a secure means, and information propagator will air the info to a replacement cluster of users if the attributes satisfy the access policies within the ciphertext. We have a tendency to additional gift a multiparty access management mechanism over the disseminated ciphertext, within which the info co-owners will append new access policies to the ciphertext thanks to their privacy preferences. Moreover, 3 policy aggregation methods, as well as full allow, owner priority and majority allow, are provided to solve the privacy conflicts drawback caused by totally different access policies. The safety analysis and experimental results show our theme is sensible and economical for secure information sharing with multi-owner in cloud computing.

Keywords: Multi-Cloud storage, Proof of Storage, Cloud Computing, Third Party Auditor.

I. INTRODUCTION

The conspicuousness of appropriated processing is procured from the benefits of rich accumulating resources and second access. It adds up to the advantages of figuring system, and thereafter gives on-demand benefits over the Internet. Various famous associations are directly giving open cloud organizations, for instance, Amazon, Google, and Alibaba. These organizations license particular customers and attempt customers to move data (for instance photos, chronicles and files) to cloud pro association (CSP), to get to the data at whatever point wherever and offering the data to others. To guarantee the security of customers, most cloud organizations achieve access control by keeping up access control list (ACL). In this way, customers can choose to either circulate their data to anyone or grant access rights just to their avowed people. In any case, the security dangers have brought stresses up in people, as a result of the data is taken care of in plaintext structure by the CSP. At the point when the data is posted to the CSP, it is out of the data owner's control.

Lamentably, the CSP is generally a semi-confided in worker which genuinely follows the assigned convention, yet may gather the clients' information and even use them for benefits without clients' assents. Then again, the information has huge uses by different information customers to become familiar with the conduct of users. Actually, these encryption strategies can forestall unapproved substances (for example semi-trusted CSP and malevolent clients) from getting to the information, however it may not consider information dispersal in cloud computing. However, consolidating security inclinations of information proprietor and various co-proprietors isn't a simple assignment; because of protection struggle is unavoidable in multiparty approval authorization. Protection strife happens when the co proprietors have inverse security approaches, and it brings about information being inconceivably gotten to with anybody. To manage this difficulty, multiparty access control systems (for example casting a ballot conspire) are additionally given. Nonetheless, every one of them depend on plaintext information. In this paper, we propose a character based secure information bunch sharing and contingent spread plan with multi-proprietor in distributed computing.

Be that as it may, when the data is encoded with the above procedures, information disseminators aren't ready to adjust the ciphertext transferred by information owners[13]. Intermediary re-encryption (PRE) conspire [14] is used to accomplish secure information spread in cloud computing by designating a re-encryption key identified with the new recipients to the CSP. Be that as it may, the information disseminator can scatter the entirety of the information proprietor's data to others with this re-encryption key, which can't meet the reasonable necessity since the data proprietor may just permit the information disseminator to disperse a particular record.

A refined idea referenced as contingent PRE (CPRE) [15, 16] could address this issue, during which data owner can uphold re-encryption authority over the initial ciphertexts and just the ciphertexts fulfilling specific condition are regularly re-scrambled with comparing re-encryption key. In any case, customary CPRE plans only support basic catchphrase conditions, all together that they can't coordinate complex circumstances in distributed computing great. so as to support expressive conditions rather than catchphrases, characteristic based CPRE is proposed [17], which conveys an access strategy inside the ciphertext. The re-encryption keys related with a gathering of qualities, hence the intermediary can re-encrypt

the ciphertext just the re-encryption key matches the entrance strategy. During thusly, information proprietor can alter fine-grained spread condition for the shared information. For instance, information proprietor permits project managers inside the association to disperse the progress report in OneDrive, while just allow leader directors in account office to scatter the undertaking financial plan in OneDrive during a chose timeframe.

Other than the need of restrictive information scattering, multiparty access control issue for information partaking in distributed computing like cloud joint effort and cloud-based interpersonal organizations goes along [18, 19], which recommends the unique approval necessities from various related clients are regularly obliged together to direct the common information. Consider a model where a co-composing report or a co-photograph in distributed computing with three clients, Alice, Bob, and Carol. On the off chance that Alice who is that the information proprietor transfers this co-composing record or co photograph to the CSP and labels both Bob and Carol in light of the fact that the co-owners. Alice can confine this information to be scattered to a specific gathering of clients, while the co-proprietors Bob and Carol may have distinctive protection worries about this information. It's colossal and high security issue if applying the inclination of only one gathering, which can make such information, be imparted to undesired beneficiaries. (For example casting a ballot conspires) are additionally given. In any case, every one of them are upheld plaintext information.

II. RELATED WORK

A series of unaddressed security and privacy issues emerge as important research topics in cloud computing. To deal with these threats, appropriate encryption techniques should be utilized to guarantee data confidentiality. In private information sharing schemes, information owner outsources encrypted information to the CSP by shaping a listing of receivers, therefore solely the suppose dusers within the list will get the cryptography key and further decode the non-public information. ABE is another promising one-to-many science technique to understand information encryption and fine-grained access management in cloud computing. Secure data dissemination is another important security requirement for data storage in cloud computing. The identity-based PRE is a basic encryption algorithm to reach secure data dissemination in cloud computing, with which the data disseminators could send their re-encryption keys to the semi-trusted proxy to transform data owner's ciphertext for new users

III. ATTRIBUTE- BASED ENCRYPTION

Attribute based encryption might be a kind of open key encryption during which the key of a client and hence the ciphertext are needy upon traits (for example the nation during which he lives, or the sort of membership he has). In such a framework, the unscrambling of a ciphertext is attainable as long as the arrangement of characteristics of the client key matches the properties of the ciphertext.
An urgent security part of trait based encryption is plot opposition: An enemy that holds numerous keys should possibly be prepared to get to information if at least one individual key award gets to.

IV. IDENTITY BASED BROADCAST ENCRYPTION

Communicate encryption empowers a supporter to encode messages and transmit them to some subset S of approved clients. In personality based communicate encryption conspires; a telecom sender normally scrambles a message by joining open characters of recipients in S and framework parameters. An IBBE plot includes a position: the Private Key Generator (PKG). The PKG allows new individuals ability of decoding messages by giving each new part (with character IDi) an unscrambling key skIDi. The age of skIDi is performed utilizing an ace mystery key MSK. The supporter scrambles messages what's more, transmits these to the gathering of clients by means of the communicate

DOI 10.17148/IJARCCE.2021.10305

channel. In an (open key) IBBE encryption conspire, the supporter doesn't hold any private data and encryption is performed with the assistance of an open key PK what's more, personalities of the beneficiaries. Following the KEM-DEM philosophy, communicate encryption is seen as the mix of a particular key epitome instrument (a Broadcast-KEM) with a symmetric encryption (DEM) that will stay certain all through the paper.

V. CONCLUSION

The information security and protection is a worry for clients in distributed computing. Specifically, how to uphold security worries of various proprietors and ensure the information privacy turns into a test. In this paper, we present a protected information bunch sharing and restrictive scattering plot with multi-proprietor in distributed computing. In our conspire, the information proprietor could scramble her or his private information and offer it with a gathering of information accessors at one time in a helpful manner dependent on IBBE method. Then, the information proprietor can determine fine-grained admittance strategy to the ciphertext dependent on quality based CPRE, subsequently the ciphertext must be re-scrambled by information disseminator whose qualities fulfill the entrance strategy in the ciphertext. We further present a multiparty access control system over the ciphertext, which permits the information co-proprietors to add their entrance strategies to the ciphertext. Plus, we give three strategy collection systems including full license, proprietor need and greater part grant to tackle the issue of protection clashes.

ACKNOWLEDGMENT

I profoundly grateful to **Prof. B.R.Solunke**. for his/her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. I would like to express my deepest appreciation towards **Principal S. D. Navale**, **HOD V.V. Pottigar** department of computer engineering and PG coordinator B.R. Solunke sir. I must express my sincere heartfelt gratitude to all staff members of computer engineering department who helped me directly or indirectly during this course of work. Finally, I would like to thank my family and friends, for their precious support.

REFERENCES

[1]. J. Be then court, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” Proc. IEEE Symposium on Security and Privacy (SP ‘07), pp. 321-334, 2007.

[2]. C. Delerabl´ee, “Identity-based broadcast encryption with constant size ciphertextsand private keys,” Proc. International Conf. on the Theory and Application of Cryptologyand Information Security (ASIACRYPT ‘2007), pp. 200-215, 2007.

[3]. L. Jiang, and D. Guo “Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage,” IEEE Access, vol. 5, pp. 13336– 13345, 2017.

[4]. B. Lang, J.Wang, and Y. Liu, “Achieving flexible and self-contained data protection in cloud computing,” IEEE Access, vol. 5, pp. 1510- 1523, 2017.

[5]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang,“A secure and efficient ciphertext-policy attribute-based proxy re-encryption for clouddata sharing,” Future Generation Computer Systems, vol. 52, pp. 95-108, 2015.

[6]. L. Liu, Y. Zhang, and X. Li,“KeyD: secure key-deduplication with identity-basedbroadcast encryption,” IEEE Transactions on Cloud Computing, 2018.

[7]. N. Paladi, C. Gehrmann, and A. Michalas, “Providing user security guarantees inpublic infrastructure clouds,” IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp.405-419, 2017.

[8]. K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, “Combining data owner-side and cloud-side access control for encrypted cloud storage,” IEEE Transactions on InformationForensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[9]. Z. Yan, X. Li, M.Wang, and A. V. Vasilakos, “Flexible data access control based on trust and reputation in cloud computing,” IEEE Transactions on Cloud Computing, vol.5, no. 3, pp. 485-498, 2017.

[10]. Q. Zhang, L. T. Yang, and Z. Chen,“Privacy preserving deep computation modelon cloud for big data feature learning,” IEEE Transactions on Computers, vol. 65, no. 5,pp. 1351-1362, 2016.

[11]. X. Li, Y. Zhang, B. Wang, and J. Yan, “Mona: secure multi-owner data sharing fordynamic groups in the cloud,” IEEE Transactions on Parallel and Distributed Systems,vol. 24, no. 6, pp. 1182 – 1191, 2013.

[12]. K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, “My privacy my decision: control ofphoto sharing on online social networks,” IEEE Trans. on Dependable and Secure Computing,vol. 14, no. 2, pp. 199-210, 2017.

[13]. L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, “Trust-based collaborative privacy

DOI 10.17148/IJARCCE.2021.10305

Management in online social networks," IEEE Transactions on Information Forensicsand Security, vol. 14, no. 1, pp. 48- 60, 2019.

[14]. C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (withshort ciphertexts)," Proc. 28th Ann. International Conf. on Advances in Cryptology: theTheory and Applications of Cryptographic (EUROCRYPT '09), pp. 171-188, and 2009.

[15]. Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.

[16]. S. Patranabis, Y. Shrivastava, and D.Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud," IEEE Transactions on Computers, vol. 66, no. 5, pp. 891–904, 2017

[17]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption forfine-grained access control of encrypted data," Proc. 13th ACM Conf. on Computer andCommunications Security (CCS '06), pp.89- 98, 2006.

[18] X. Li, Y. Zhang, B. Wang, and J. Yan, "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, 2013.

[19] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online social networks," IEEE Trans. On Dependable and Secure Computing, vol. 14, no. 2, pp. 199-210, 2017.

[20] K. Thomas, C. Grier, and D. M. Nicol, "UnFriendly: multi-party privacy risks in social networks," Proc. International Symposium on Privacy Enhancing Technologies Symp. (PETS '2010), pp. 236-252, 2010.

[21] L. Fang, L. Yin, Y. Guo, Z. Wang, and Fenzhua Li, "Resolving access conflicts: an auction-based incentive approach," Proc. IEEE Military Communications Conference (MILCOM), pp. 1-6, 2018.

[22] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 48-60, 2019.

[23] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," Proc. 28th Ann. International Conf. on Advances in Cryptology: the Theory and Applications of Cryptographic (EUROCRYPT '09), pp. 171-188, and 2009.

[24] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.

[25] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud," IEEE Transactions on Computers, vol. 66, no. 5, pp. 891–904, 2017.

[26] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. 24th Ann. International Conf. on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), pp. 457-473, 2005.

[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. on Computer and Communications Security (CCS '06), pp.89-98, 2006.

[28] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute based data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.

[29] L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving social assisted mobile content dissemination scheme in DTNs," Proc. 32nd IEEE International Conf. on Computer Communications (INFOCOM '2013), pp. 2301-2309, 2013.

[30] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attribute based access control with constant-size ciphertext in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp. 617-627, 2017.

[31] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attribute-based access control," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130-2145, 2018.

[32] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," IEEE Access, vol. 6, pp. 9114-9128, 2018.

[33] M. Green and G. Ateniese, "Identity-based proxy re-encryption," Proc.5th International Conf. on Applied Cryptography and Network Security (ACNS '07), pp. 288-306, 2007.

[34] Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu, and Y. Ding, "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," Future Generation Computer Systems, vol. 62, pp. 128-139, 2016.

[35] J. Weng, R. H. Deng, X. Ding, C. K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in Proc. of 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09), pp. 322-332, 2009.