International Journal for Modern Trends in Science and Technology, 8(09): 127-130, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809025
Available online at: http://www.ijmtst.com/vol8issue09.html

Comfortable Information Institution Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing

K Lokesh[1] | K Lakshmana Reddy[2]

[1]Master of Computer Applications (MCA), SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
K Lokesh and K Lakshmana Reddy. Comfortable Information Institution Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 127-130. https://doi.org/10.46501/IJMTST0809025

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

With the rapid improvement of cloud offerings, big volume of records is shared via cloud computing. despite the fact that cryptographic strategies had been utilized to provide statistics confidentiality in cloud computing, contemporary mechanisms cannot enforce privacy concerns over cipher textual content related to a couple of owners, which makes co-proprietors unable to accurately manipulate whether or not statistics disseminators can in reality disseminate their information. on this paper, we advocate a cozy facts group sharing and conditional dissemination scheme with multi-proprietor in cloud computing, in which information owner can percentage personal records with a set of users thru the cloud in a comfortable manner, and records disseminator can disseminate the facts to a brand new institution of customers if the attributes fulfill the get right of entry to rules inside the cipher text. We similarly gift a multiparty access manage mechanism over the disseminated cipher text, wherein the statistics co-owners can append new get right of entry to rules to the cipher textual content due to their privacy possibilities. moreover, three coverage aggregation techniques, which includes full permit, proprietor priority and majority permit, are provided to resolve the privateness conflicts hassle as a result of one of a kind get admission to policies. the safety evaluation and experimental consequences show our scheme is sensible and green for cozy facts sharing with multi-proprietor in cloud computing.

Keywords: Data sharing, cloud computing, conditional proxy re-encryption, attribute-based encryption

1. INTRODUCTION

Reputation of cloud computing is obtained from the blessings of rich garage assets and immediately get entry to . It aggregates the resources of computing infrastructure, after which presents on-demand offeringsover the net. Many famous businesses at the moment are imparting public cloud services, along with Amazon, Google, Alibaba.

These services permit character customers and corporation customers to upload records (e.g. photographs, motion pictures and files) to cloud provider provider (CSP), for the motive of getting access to the records at any time anywhere and sharing the data with others. a good way to defend the privacy of users, maximum cloud offerings acquire get admission to manipulate by way of maintaining get entry to manage

list (ACL). on this manner, customers can select to both publish their facts to all of us or furnish access rights merely to their accepted human beings. but, the safety risks have raised concerns in people, due to the information is stored in plaintext form with the aid of the CSP. as soon as the facts is published to the CSP, it is out of the records owner's control . alas, the CSP is often a semi-relied on server which truly follows the certain protocol, but would possibly accumulate the customers' information or even use them for benefits with out customers' sees eye to eye.

Then again, the facts has notable usages by means of diverse records purchasers to research the conduct of customers . these security troubles motivate the powerful answers to shield facts confidentiality. it's miles crucial to undertake get right of entry to manage mechanisms to acquire cozy facts sharing in cloud computing . currently, cryptographic mechanisms such as attribute-based totally encryption (ABE) , identification- primarily based broadcast encryption (IBBE) , and remote attestation were exploited to settle those safety and privateness issues. ABE is one of the new cryptographic mechanisms used in cloud computing to attain relaxed and satisfactory-grained information sharing . It functions a mechanism that enables an get entry to control over encrypted facts the usage of access rules and ascribed attributes amongst decryption keys and cipher texts.

2. LITERATURE SURVEY

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. By utilizing the IBBE technique [23], Huang et al. [24], Patranabis et al. [25] and Liu et al. [9] proposed several private data sharing schemes in cloud computing. In these schemes, data owner outsources encrypted data to the CSP by defining a list of receivers, thus only the intended users in the list can get the decryption key and further decrypt the private data. ABE is another promising one-to-many cryptographic technique to realize data encryption and fine-grained access control in cloud computing [26, 27]. Specially, ciphertext-policy ABE (CP-ABE) is suited for access control in real world applications due to its expressiveness in describing the access policy of ciphertext [28].

Secure data dissemination is another important security requirement for data storage in cloud computing. The identity-based PRE [33] is a basic encryption algorithm to reach secure data dissemination in cloud computing, with which the data disseminators could send their reencryption keys to the semi-trusted proxy to transform data owner's ciphertext for new users [34]. Further, attribute- based PRE [17] has been employed in cloud computing by incorporating the ABE technique. The proxy can transform the ciphertext under an access policy into the one under another access policy with data disseminator's re-encryption key, and the users who satisfy the new access policy can access the plaintext. However, the above PRE schemes only allow data dissemination in an all-ornone manner. This issue is further addressed by CPRE scheme [35], in which the proxy can successfully reencrypt the ciphertext only if the prescribed conditions are met. However, in earlier CPRE schemes [35, 36], the conditions are keywords only, which would limit the flexibility when enforcing complex delegations in cloud computing. Yang et al. [37] proposed an attribute-based CPRE scheme by deploying an access policy in a ciphertext generated by public-key encryption. The reencryption key is generated by the secret key associated with a set of attributes, which allows the proxy to reencrypt the ciphertext only when these attributes satisfy the access policy. Wang et al. [38] proposed a preauthentication approach for sharing data in cloud, which achieves receiver's attribute authentication before the reencryption operation.

3.PROBLEM STATEMENT

`The device model consists of the subsequent entities, as shown 1) relied on authority: The trusted authority is a fully trusted element that initializes the device public key, and generates non-public keys in addition to characteristic keys for users.

As an instance, it may be acted by way of the administrator of the business enterprise [18] or social safety administration [44].

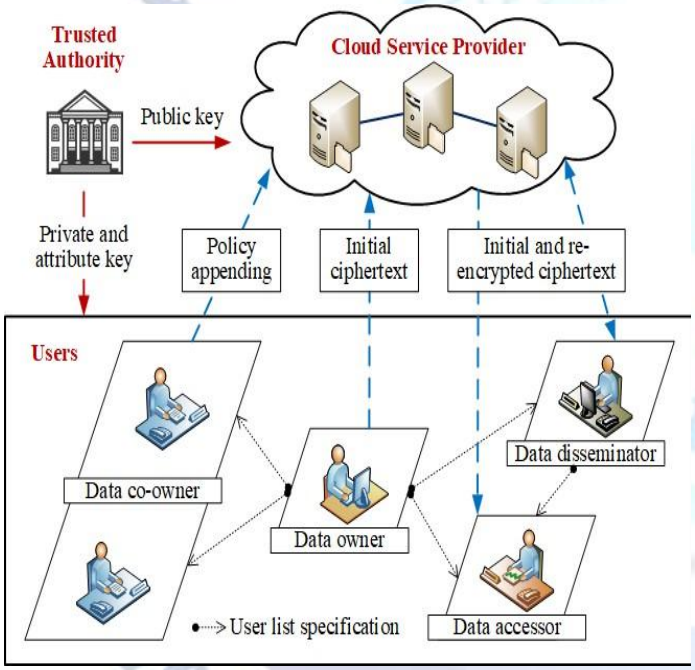
2) CSP: The CSP is a semi-relied on component that gives every person with a digital area and convenient data storage service with the cloud infrastructure. It additionally appends get entry to regulations to the

ciphertexts for records co-proprietors andgenerates re-encrypted ciphertexts for customers.

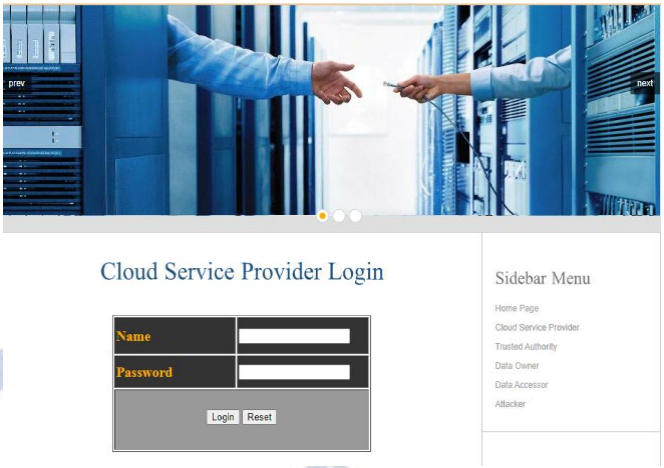
3) user: We divide the person function into the subsequent categories:data proprietor, statistics co-proprietor, statistics disseminator and records accessor. The statistics owner can pick out a coverage aggregation strategy and define an get right of entry to coverage to enforce dissemination conditions. Then he encrypts statistics for

a set of receivers, and outsources the ciphertext to CSP for sharing and dissemination. The statistics co-proprietors tagged by using facts owner can append get entry to policies to the encrypted records with CSP and generate the renewed ciphertext.

4. ARCHITECHTURE



5. RESULTS



6. CONCLUSION

The data safety and privacy is a situation for customers in cloud computing. especially, the way to put into effect privateness issues of more than one owners and guard the information confidentiality will become a mission. on this paper, we gift a comfy facts institution sharing and conditional dissemination scheme with multi-owner in cloud computing. In our scheme, the records proprietor ought to encrypt her or his private records and percentage it with a co006Clection of records accessor at one time in a handy way based on IBBE technique. meanwhile, the records owner can specify fine-grained get admission to policy to the cipher text based totally on attribute-based totally CPRE, accordingly the cipher text can simplest be re encrypted by using facts disseminator whose attributes fulfill the get entry to policy in the cipher textual content. We in addition present a multiparty get right of entry to manage mechanism over the cipher textual content, which lets in the records co-proprietors to append their get admission to regulations to the cipher text. besides, we provide three coverage aggregation strategies along with full allow, owner priority and majority allow to solve the problem of privatenessconflicts.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] 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.

[2] 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.
[3] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1351-1362, 2016.
[4] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.
[5] 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 Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.
[6] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT '2007), pp. 200-215, 2007.
[7] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.
[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," Proc. IEEE Symposium on Security and Privacy (SP '07), pp. 321-334, 2007.
[9] L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," IEEE Transactions on Cloud Computing, 2018, https://ieeexplore.ieee.org/document/8458136.
[10] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee. org/document/8395392.
[11] Box, "Understanding collaborator permission levels", https://community. box.com/t5/Collaborate-By-Inviting-Others/Understanding-Collaborator-Permission-Levels/ta-p/144.
[12] Microsoft OneDrive, "Document collaboration and co-authoring", https://support.office.com/en-us/article/document-collaborationa nd-co-authoring-ee1509b4-1f6e-401e-b04a-782d26f564a4.
[13] H. He, R. Li, X. Dong, and Z. Zhang, "Secure, efficient and finegrained data access control mechanism for P2P storage cloud," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, 2014.
[14] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloud computing," IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee.org/document/7448446.
[15] J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloud environment," Proc. of 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 541–546, 2014.
[16] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based non conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.
[17] 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 cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95-108, 2015.
[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, 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

Authors Biography

K Lokesh currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. His research interests include Data Structures, WebTechnologies, Operating Systems and Data Science and Artificial Inteligence

K.Lakshamana Reddy is working as Associate Professor in SVKP & Dr K S Raju Arts & Science College,Penugonda,West Godavari District, A.P. He received MCA from Andhra University, 'C' level from DOEACC, New Delhi and M.Tech from Acharya Nagarjuna University, A.P. He attended and presented papers in conferences and seminars. He has done online certifications in several courses from NPTEL. His areas of interests include Computer Networks, Network Security and Cryptography, Formal Languages and Automata Theory and Object Oriented programming languages.