ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

A Survey on Secure Group Sharing and Fine Grained Conditional Distribution

Prof. Rokade.S.M[1], Jondhale Dhanashree Rajaram[2]

Department of Computer Engineering, Pravara Rural Engineering College, Loni Pravara, Ahmednagar, Maharashtra, India [1,2]

ABSTRACT: Cloud computing is becoming a prominent computing paradigm that allows users to store their data into a cloud server to enjoy scalable and on-demand services. Group data sharing in cloud environments has become a hot topic in recent. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. Although encryption techniques have been used to provide data confidentiality and data security in cloud computing, current technique cannot enforce privacy concerns over encrypted data associated with multiple data owners, which makes co-owners unable to appropriately control whether data distributor can actually distribute their data. In this paper, we propose an Efficient and secure data group sharing and conditional distribution scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data distributor can distribute the data to a new group of users if the attributes satisfy the access policies in the encrypted data.

KEYWORDS: Data Sharing, Conditional Proxy Re-Encryption, Attribute-Based Encryption, Privacy Conflict, System Attackability, Remote Synchronization, Distribution and Optimization

.

I. INTRODUCTION

Cloud systems can be used to enable data sharing capabilities and this can provide several benefits to the user and organization when the data shared in cloud. Since many users from various organizations contribute their data to the Cloud, the time and cost will be less compared to manually exchange of data. Google Docs provides data sharing capabilities as groups of students or teams working on a project can share documents and can team up with each other successfully. This allows higher productivity compared to previous methods of frequently sending updated versions of a document to members of the group via email attachments. People are expecting data sharing capability on their computers, phones and laptop etc. People love to share their information with others such as family, colleagues, friends or the world. Students also get benefit when working on group projects, as they are able to team up with members and get work done efficiently.

CSPs such as Dropbox, among many others, employ sync-like protocols [7] to synchronize the local file to remote file in their centralized clouds [8]. Every local file is partitioned into small chunks and these chunks are hashed with fingerprinting algorithms such as SHA-1, MD5. Thus, a file's contents can be uniquely identified by this list of hashes. For each update of local file, only chunks with changed hashes will be uploaded to the cloud. In order to protect the privacy of users, most cloud services achieve access control by maintaining Access Control List (ACL). In this way, users can choose to either publish their data to anyone or grant access rights merely to their approved people. However, the security risks have raised concerns in people, due to the data is stored in plaintext form by the CSP. Once the data is posted to the CSP, it is out of the data owne's control.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to-many pattern. As the data shared on the cloud is valuable, various security methods are provided by cloud. In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption]. Symmetric-key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology. In existing system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack. Another gap is that a user is not allowed to upload multiple files of same name.

II. LITERATURE SURVEY

They made [1], a framework for Ciphertext-Policy Attribute Based Encryption. Our framework takes into consideration another sort of encoded get to control where client's private keys are specified by a lot of qualities and a gathering scrambling information can determine a strategy over these qualities indicating which clients can decode. Our framework permits strategies to be communicated as any monotonic tree get to structure and is impervious to intrigue assaults in which an assailant may acquire numerous private keys. At long last, we gave a usage of our framework, which incorporated a few enhancement methods. Intermediary based, [2] numerous cloud capacity framework that for all intents and purposes tends to the unwavering quality of the present cloud reinforcement stockpiling. NCCloud not just gives adaptation to internal failure away, yet in addition permits practical fix when a cloud for all time falls flat. NCCloud executes a viable adaptation of the FMSR codes, which recovers new equality pieces during fix subject to the necessary level of information excess. Our FMSR code usage dispenses with the encoding necessity of capacity hubs (or cloud) during fix, while guaranteeing that the new arrangement of put away lumps after each round of fix jam the necessary adaptation to non-critical failure. Our NCCloud model shows the viability of FMSR codes in the cloud reinforcement use, as far as money related expenses and reaction times. The Internet of Things (IoT) [3], gadgets continually create information, and require the information examination to be fast, which can't be given by the conventional distributed computing design. With the objective of breaking down the IoT information near the gadgets that create and work on the information, edge figuring has been acquainted for the expansion with the edge of the system from distributed computing. Despite the fact that edge registering encourages distributed computing in tending to the inertness issue of information handling, it likewise brings greater security and protection issues to the current distributed computing system. Because of the reality that Property Based Encryption (ABE) underpins fine-grained (or versatile) get to control for information things in scrambled structures, ABE has been generally accepted to be a perfect answer for ensure information security and protection for situations of distributed computing. To accomplish fine-grained get to control for the edge figuring condition, in this paper, we proposed an idea named intermediary supported Ciphertext-Approach Characteristic Based Encryption (PA- CPABE). Subsequent to portraying a conventional development of PA-CPABE, we officially examined its security. What's more, we displayed and actualized a launch of PA-CPABE to assess its proficiency.

In this paper [4], we propose a secure exchange of data groups and conditional spreading scheme with multiple owners in cloud computing, where the data owner can share private data with a group of users through the cloud in a secure way and the data communicator can disclose the data to a new group of users if the attributes satisfy the access criteria in the encrypted text. We also present a multipart access control mechanism on the Transmit encrypted text, where data owners can add new policies to access encrypted text due to their privacy preferences In addition, three policy aggregation strategies are provided, including full authorization, owner priority and majority authorization to solve the problem of privacy conflicts caused by different access policies. Safety analysis and experimental results show our scheme is practical and efficient for the secure exchange of data with multiple owners in cloud computing. In this paper [5], we propose a scheme to check the data access to cloud computing based on data-driven trust owner and reputation generated by a series of reputation it focuses flexibly by applying attributes Encryption and proxy encryption. We integrate the concept of trust assessment and reputation aware of the context in a cryptographic system to support multiple controls scenarios and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

strategies. The safety and performance of ours the schemes are evaluated and justified by an exhaustive analysis, Safety testing, comparison and implementation. The results shown the efficiency, flexibility and flexibility of our data scheme access control in cloud computing.

In this paper [6], propose a notion called a proxy-assisted encrypted text policy Attribute-based encryption (PA-CPABE), which outsources most decryption calcula3 A General Framework for Edited Video and Raw Video Summarization tions to peripheral devices. Respect For the existing ABE with outsourced decryption schemes (ABE-OD), PA-CPABE has the advantage that the distribution of keys It does not require any secure channel. We present a generic construction of PA-CPABE and therefore we demonstrate its security. Moreover, we implement an instance of the proposed PA-CPABE framework to evaluate its performance. In this paper [7], propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present two protocols for different settings, followed by performance and security analysis. In this paper [8], describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. We continue with an extensive theoretical analysis with proofs about protocol resistance against attacks in the defined threat model.

The protocols allow trust to be established by remotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality of data in remote storage, with encryption keys maintained outside of the IaaS domain. Presented experimental results demonstrate the validity and efficiency of the proposed protocols. The framework prototype was implemented on a test bed operating a public electronic health record system, showing that the proposed protocols can be integrated into existing cloud environments. In this paper [9], propose an identity based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a reencryption key to cloud server. The re-encryption conditions are associated with attributes and releasing time, which allows data owner to enforce fine-grained and timed-release access control over disseminated cipher texts. The theoretical analysis 4 Department of Computer Engineering (2019-2020) A General Framework for Edited Video and Raw Video Summarization and experimental results show our proposed scheme makes a tradeoff between computational overhead and expressive dissemination conditions.

In this paper [10], based on conditional proxy broadcast re-encryption technology, an encrypted data sharing scheme for secure cloud storage is proposed. The scheme not only achieves broadcast data sharing by taking advantage of broadcast encryption, but also achieves dynamic sharing that enables adding a user to and removing a user from sharing groups dynamically without the need to change encryption public keys. Moreover, by using proxy re-encryption technology, our scheme enables the proxy (cloud server) to directly share encrypted data to the target users without the intervention of data owner while keeping data privacy, so that greatly improves the sharing performance. Meanwhile, the correctness and security is proved, the performance is analyzed and the experimental results are shown to verify the feasibility and efficiency of the proposed scheme. In this paper [11], they attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.

II. DYNAMIC SECURE GROUP SHARING

Zhongma Zhu and Rui Jiang [1] (2016), proposed a secure anti collision data sharing scheme for dynamic groups. The group manager takes charge of user registration and user revocation. Group members are a set of registered users. They will store their own data into the cloud and share them with others. They proposed a secure way of key distribution without any secure channels. The users can obtain their private keys from group manager without any Certificate Authorities, due to the verification for the public key of the user. Since there are no secure communication channels between communication entities, the information can be protected from passive eavesdroppers. The proposed scheme achieved finegrained access control. This allowed any user in the group to use the source in the cloud and the revoked users cannot access the cloud again after they are revoked. This scheme protects from collusion attack and provides a secured user revocation, so the revoked users cannot get the original data file. It supports dynamic groups efficiently. So, previous users need not update their private keys when a new user joins the group or when a user is revoked from the group. The design goals of this scheme include key distribution, data confidentiality, access control and efficiency. Kaiping Xue [5] (2014) proposed a dynamic secure group sharing framework in public cloud computing environment. This framework combines proxy re-encryption, enhanced Treebased Group Diffie-Hellman (TGDH) and proxy signature together into a protocol. By applying the proxy signature technique, the group leader can give rights to group management to choose one or more groups members, all the session key are protected in the digital envelopes and all the data sharing files are safely stored in Cloud Servers. The improved TGDH scheme is to dynamically modify a group key pair when they are in group ,leaving the group or joining the group as well as its does not require all of the group members been online all the time. Based on proxy re-encryption, most data processing operations can be assigned to Cloud Servers without reveal any private information. Advantages of this proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing. Xuefeng Liu [4] (2013) proposed a secure data sharing design for dynamic groups in an untrusted cloud. In this design, a user can share data with others in the group without revealing identity privacy to the cloud. Its supports efficient user revocation, which can be achieved through a public revocation list without modifying the private keys of the remaining users, and new users join can directly decrypt files stored in the cloud before their participation. This scheme guarantees efficiency as well as encryption computation costs are constant.

III. CONCLUSION

Distributing knowledge on multiple clouds provides users with a certain degree of data run management there in no single cloud supplier are aware of the entire user's knowledge. However, unplanned distribution of information chunks will cause avoidable information run. The data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the data confidentiality becomes a challenge. The problem with data sharing in the cloud is the privacy and security issues. Various techniques are discussed in this paper to support privacy and secure data sharing such as Data sharing with forward security, secure data sharing for dynamic groups, Attribute based data sharing, encrypted data sharing, Shared Authority Based Privacy-Preserving Authentication Protocol for access control of outsourced data. The study concludes that secure anti collision data sharing scheme for dynamic groups provides more efficiency, supports access control mechanism and data confidentiality to implement privacy and security in dynamic group sharing. There is more scope for future research in the field of secure data sharing for dynamic groups.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

REFERENCES

[1] 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.

[2]. H. Chen, Y. Hu, P. Lee, and Y. Tang, "Nccloud: A network-coding-based storage system in a cloud-of-clouds," 2013.

[3]. 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.

[4]. 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.

[5] Qinlong Huang, Member, IEEE, Yixian Yang, Wei Yue and Yue He" Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing", IEEE TRANSACTIONS ON CLOUD COMPUTING , APRIL 2019.

[6] 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.

[7] 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.

[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 Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[9] 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.

[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.

[11] 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.