JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

Multi-Owner Information Collection and Dependent Distribution in a Distributed Computation Environment

A. Lakshmi Parvathi #1, P. L. S. Amulya #2, Shaik. Karimoon #4, L. Deepak Sai Reddy #5, L. Rahul #6

#1 Asst. Professor, Department of Computer Science and engineering

#2,3,4,5,6 B.Tech., Scholars, Department of Computer Science and engineering

Qis College of Engineering and Technology

Abstract- As cloud services continue to evolve, they are increasingly being used to send massive volumes of data across the internet. Existing procedures are not able to enforce privacy concerns over cypher text connected with many owners, despite the use of cryptographic techniques to ensure data secrecy in cloud computing. Consequently, there is a lack of confidence among co-owners that data disseminators would exercise appropriate care in deciding whether or not to share their data. A data owner may safely exchange data with a group of users through the cloud, and a data disseminator can disseminate the data to a new group of users provided the characteristics fulfil the access rules in the cypher text, as proposed in this work. The data co-owners may add new access rules to the cypher text depending on their privacy choices, and we also propose a multiparty access control mechanism over the disseminated cypher text. Also included are three policy aggregation solutions for dealing with privacy conflicts caused by different access policies: the complete permit, the owner priority, and the majority permit. Our security analysis and practical findings show that our approach is both effective and efficient for multi-owner safe data sharing in the cloud.

Keywords— Multi-Owner, collection, dependence, cloud, distributed computing.

I. INTRODUCTION

The advantages of cloud computing, such as ample storage space and easy accessibility, have contributed to its meteoric rise in popularity [1]. It pools the power of existing data centres to meet the demand for "cloud" services delivered through the web. Public cloud services are being provided by several well-known firms. Individuals and businesses alike may take use of these services to store data (such as images, videos, and documents) with a cloud service provider (CSP) from which it can be retrieved and shared at any time and from any location. Most cloud services accomplish access control by keeping an access control list, which is intended to safeguard user privacy (ACL). Users have the option of making their information publicly available or restricting it to just those they authorise. People are understandably worried about security since the CSP stores the data in unencrypted. The data owner loses all rights to the data after it has been uploaded to the CSP [2]. The CSP is often a semi-trusted server that faithfully executes the specified protocol but may secretly gather and profit from users' information without their knowledge or agreement.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

However, the data has enormous value for many other types of data consumers looking to get insight into user behaviour [3]. These vulnerabilities spur the development of workable safeguards for sensitive data. For data sharing in the cloud to be safe, it is crucial to include systems for controlling who may access what [4]. In order to solve these security and privacy issues, cryptographic algorithms including attribute-based encryption (ABE) [5], identity-based broadcast encryption (IBBE) [6], and remote attestation [7] have been put to use. To provide private and granular data exchange in the cloud, ABE is one of the new cryptographic algorithms employed [8]. Access rules and assigned properties between decryption keys and cypher texts are used to provide this system for controlling who has access to encrypted material. To decipher the cypher text, the attribute set must conform to the policy governing access. IBBE is another widely used method in cloud computing [9, 10], allowing users to simultaneously send encrypted data to a large number of recipients while treating each recipient's public key as if it were a randomly generated string. In fact, for OR-gated policies, IBBE may be seen as a particular example of ABE. IBBE is more suited for securely broadcasting data to specified receivers in the cloud because to its low-cost key management and modest constant policy sizes, in comparison to ABE, where the secret key and cypher text are both linked to a set of characteristics. More people will feel comfortable entrusting the cloud with sensitive information if data owners can utilise identities to safely and efficiently share information with a select set of users. However, data distribution in cloud computing may not be taken into account by these encryption methods, even while they are effective at preventing unauthorised organisations (such as semi-trusted CSPs and malevolent users) from accessing the data. Data disseminators (e.g. editor and collaborator) in a cloud collaboration scenario like Box [11] and One Drive [12] may share the documents with new users, even those outside the organisation. After the data has been encrypted using the aforementioned methods, data distributors will no longer be able to alter the uploaded cypher text provided by data owners [13]. Using a re-encryption key associated with the new receivers, a proxy re-encryption (PRE) technique [14] allows for safe data transmission in cloud computing. Since the data owner may only authorise the data disseminator to disseminate a certain document, the fact that the data disseminator has access to the re-encryption key means that all of the data owner's data may be disseminated to others.

Conditional PRE (CPRE) [15, 16] is a revised approach that might solve this problem by allowing the data owner to exert re-encryption control over the original cypher texts and allowing only the cypher texts fulfilling a certain criteria to be re-encrypted with the associated re encryption key. Traditional CPRE schemes, however, only handle basic keyword conditions, which makes them poorly suited to the complicated circumstances that might arise in the cloud. Attribute-based CPRE [17] is suggested, which uses an access policy embedded in the cypher text to provide expressive conditions rather than keywords. For security reasons, the proxy can only re-encrypt the cypher text if the re-encryption key corresponds to the access policy. This allows the data owner to set very specific conditions for how the data is disseminated. Some files on One Drive, like the project budget, may be protected by their owner, who may decide to provide access to just selected individuals or groups for specified times. Data sharing in the

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

cloud, such as in cloud collaboration and cloud-based social networks [18, 19], presents a challenge for centralised access control because it must take into account the varying needs of numerous users who must all work together to manage the same pool of information. This is in addition to the requirement of conditional data dissemination. Take the scenario of Alice, Bob, and Carol working together on a document or photo in the cloud. Alice, the data owner, may upload the document or photo with Bob and Carol as co-owners if she chooses to do so when she uploads it to the CSP. While co-owners Bob and Carol may have differing privacy concerns about this data, Alice may limit its distribution to a select number of users. Applying the choice of only one party, which might lead to the data being shared with someone who shouldn't see it, is a huge and major privacy risk. Due to the inherent nature of privacy conflict in multiparty authorization enforcement [20, 21], it is not a simple process to reconcile the privacy preferences of a data owner with those of numerous co-owners.

If the data's co-owners have different expectations for how their information should be handled, a privacy conflict will arise, making sharing the information impossible [22]. Mechanisms for multi-party access control (such a vote process) are also given to help with this predicament. All of them, however, rely only on unencrypted information. In this study, we provide a multi-owner, identity-based strategy for sharing and disseminating cloud-based data securely in groups. To address these issues, we provide a method to simultaneously accomplish multi-user cypher text group sharing and capture the essential aspect of multiparty permission needs. Here are some of our scheme's benefits:

Through the use of attribute based CPRE in the cloud, we are able to accomplish fine-grained conditional distribution across the cypher text. In the first phase of deployment, the cypher text is used in conjunction with an access policy set up specifically for the data owner. Data co-owners may now accommodate their individual needs for privacy by adding new access rules to the cypher text using our suggested multiparty access control system. Accordingly, only if sufficient access rules are met by the characteristics can the cypher text be re-encrypted by the data disseminator. (2) To address the issue of privacy conflicts, we propose three solutions: (1)a complete permit, (2)owner priority, and (3)majority permit. The complete permit method requires the data disseminator to adhere to all of the access rules set out by the data owner and any co-owners. The majority permit technique requires the data owner to set a threshold value for data co-owners over which the encrypted text cannot be shared, and only then if the total of the access rules met by the characteristics of the data disseminator is higher than or equal to the defined threshold. (3) We provide proof of the validity of our strategy and then conduct experiments to assess its performance at each stage. This paper will follow the outline below. In Section 2, we survey relevant literature, and in Section 3, we provide the groundwork. Section 4 details the system model and Section 5 the policy aggregation methodologies and recommended scheme. In Section 6, we describe the system analysis, and in Section 7, we detail the findings of the experiments. In the last section of this study, we summarise our findings.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

II. RELATEDWORKS

Due to the severity of these dangers, it is imperative that proper encryption methods be used to protect sensitive information. Several confidential cloud-based data-sharing strategies have been developed by Huang et al. [24], Patranabis et al. [25], and Liu et al. [9], all of whom have relied on the IBBE method [23]. The data owner contracts the CSP to encrypt their data and provides a list of recipients; only those on the list are given access to the private data and its corresponding decryption key. When it comes to realising data encryption and granular access control in the cloud, ABE is another potential one-to-many cryptographic approach [26, 27]. Due to its richness in specifying the access policy of ciphertext [28], ciphertext-policy ABE (CP-ABE) is particularly well-suited for access control in real-world applications. Based on CP-ABE, Guo et al. [29] presented a method for disseminating data in mobile social networks that protects users' anonymity. For the purpose of protecting user anonymity while storing data in the cloud, Teng et al. [30] suggested a hierarchical CP-ABE access control mechanism. To ensure that only approved document requesters with relevant qualities are able to decrypt health records, ABE has been used in the schemes of [31] and [32] to enable access control of medical documents while delivering health services in the cloud.

Safe data sharing is another crucial aspect of cloud computing data storage security. Data disseminators can entrust a semi-trusted proxy with their reencryption keys so that the proxy can decrypt the ciphertext of the data owner and make it accessible to new users [34]. This identity-based proxy encryption algorithm (PRE) [33] is a fundamental encryption algorithm for achieving secure data dissemination in cloud computing. The ABE method has also been used in cloud computing, which is where attribute- based PRE [17] first appeared. Using the re-encryption key provided by the data disseminator, the proxy may switch the ciphertext from one access policy to another, allowing only users who meet the new access policy to see the plaintext. Data may be shared in an all-or-none fashion using the aforementioned PRE schemes, but this is currently the only option. Another solution to this problem is the CPRE scheme [35], which ensures that the proxy can only reencrypt the ciphertext successfully under certain circumstances. In contrast, the criteria in previous CPRE schemes [35, 36] are limited to keywords, which would hamper the scheme's adaptability when imposing complicated delegations in the cloud. By embedding an access policy into a ciphertext created by public-key encryption, Yang et al. [37] developed an attribute-based CPRE approach. The proxy may reencrypt the ciphertext only when the attributes meet the requirements of the access policy, and this is because the reencryption key is produced using the secret key associated with the attributes. In order to ensure that the receiver's attributes are authenticated before the reencryption process, Wang et al. [38] suggested a pre authentication method for cloud-based data exchange. For cloud computing to succeed, it is crucial that several owners exercise privacy control over their shared resources. This paper by Thomas et al. [20] demonstrates how to implement Facebook's privacy paradigm for multiparty anonymity. Users may get access to the data provided their requests comply with the exposure rules set out by the owner and other linked parties. Xu et al. [19] built a system on top of this multiparty privacy management approach to

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

provide everyone in a picture a say in how they may be seen. The aforementioned systems, however, may have a privacy conflicts issue since they don't take into account how users might really accomplish breach [39]. Such et al. [40] provided the first computational approach to settle privacy concerns between many (negotiating) users. The central concept is to determine whether user has less rigorous privacy requirements by estimating the sensitivity, relative relevance, and willingness of each item in a competing negotiation. To facilitate multi-owner data exchange while protecting individual privacy, Hu et al. [41] presented a systematic method. In order to settle the privacy disputes that arise between several parties, this plan proposes three methods based on a vote system. Unfortunately, this technique does not protect users' privacy when their data is shared with a semi-trusted CSP or by criminal users, focusing instead only on how to manage access to unencrypted data among co-owners.

Disadvantages

Privacy conflicts are unavoidable in multiparty permission enforcement, making it difficult for present work to reconcile the needs of both the data owner and any number of co-owners.

Unfortunately, the absence of conditional proxy re-encryption significantly reduces the system's security.

III. PROPOSED SYSTEM ARCHITECTURE

The suggested method presents a means to realise multi-user cypher text group sharing, hence capturing the essential aspect of multi-party permission needs. Here are some of our scheme's benefits: In cloud computing, the system uses attribute-based CPRE to provide fine-grained conditional dissemination across the encrypted text. In the first phase of deployment, the cypher text is used in conjunction with an access policy set up specifically for the data owner. Data co-owners may now accommodate their individual needs for privacy by adding new access rules to the cypher text using our suggested multiparty access control system. Therefore, only if sufficient access rules are met by the characteristics may the data disseminator re-encrypt the cypher text. To address the issue of privacy conflicts, the system gives three options for doing so: granting complete permission, giving preference to the property's owner, or granting permission by a simple majority. The complete permit method requires the data disseminator to adhere to all of the access rules set out by the data owner and any co-owners. The majority permit technique requires the data owner to set a threshold value for data co-owners over which the encrypted text cannot be shared, and only then if the total of the access rules met by the characteristics of the data disseminator is higher than or equal to the defined threshold. The system validates our scheme's validity and carries out tests to assess the scheme's efficacy by measuring its performance at each stage.

Advantages

Since data co-owners are able to update the cypher texts by adding their access rules as the dissemination conditions, data security has increased. By enforcing the data owner's access

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

policy in both the original cypher text and the refreshed cypher text, the system is made more secure via Continuous policy enforcement.

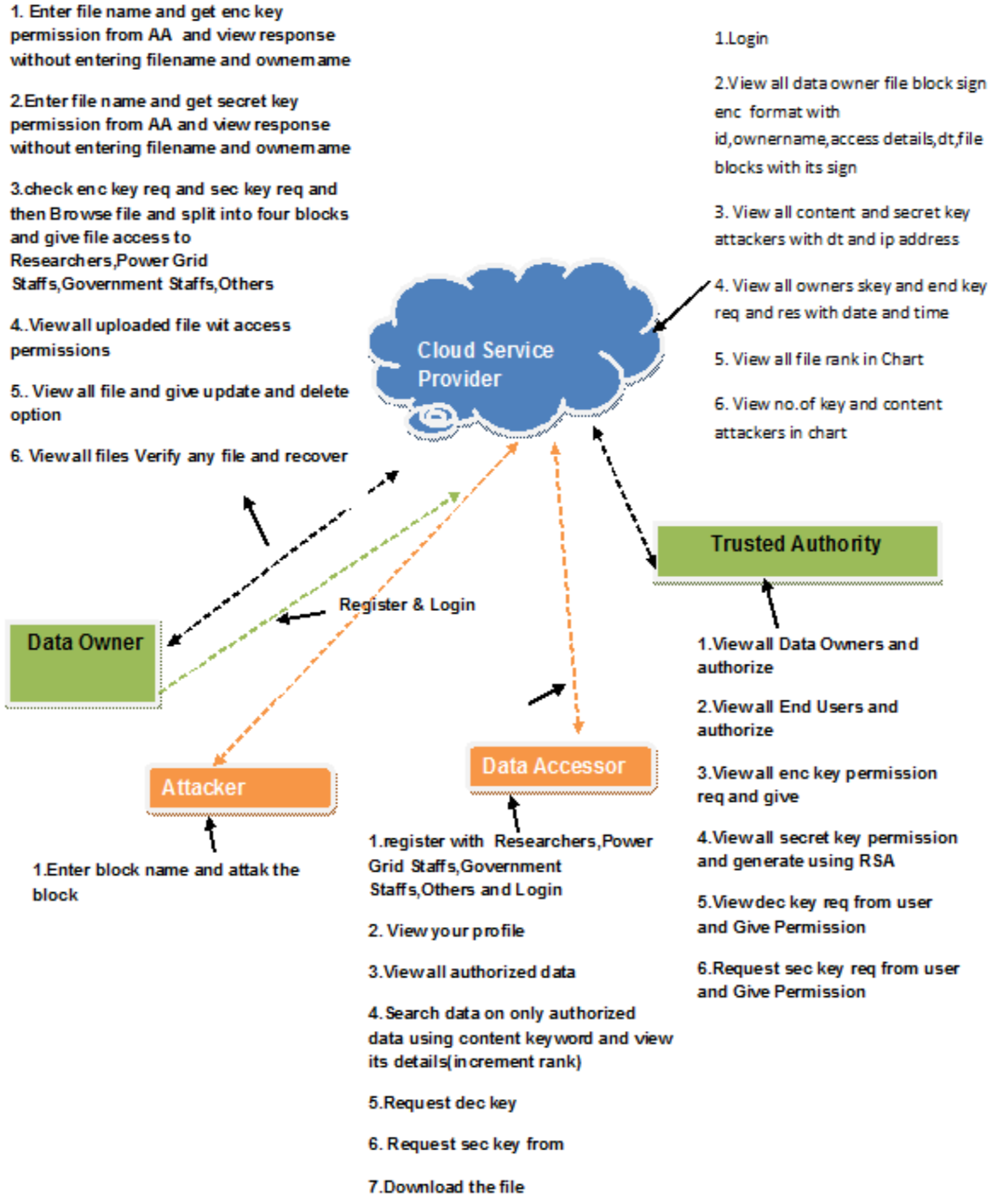

Fig.1 proposed system architecture

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

IV. RESULTS AND DISCUSSION

The output screens obtained after running and executing the system are shown in Fig.2. In this subsection, we describe how we use a pairing-based cryptography library [46] to execute our technique on a cloud server equipped with a 2.53 GHz Intel Core 2 Duo CPU and 4 GB of RAM. The public parameters are selected to offer 80 bits of security, and the elliptic curve group utilised is of type-A 160 bits, based on the supersingular curve y2 = x3 + x over a 512 bits finite field. We tried out a number of different options before settling on the Advanced Encryption Standard (AES) for our symmetric encryption needs. The data represents an average of 100 independent experiments. Before sending encrypted data to the CSP, the data owner must first establish a group of identities and an access policy. We quantify complexity by looking at how much time is spent computing and how much data is transferred. Number of accessors and characteristics in the access policy are the primary determinants of calculation time. Time required to encrypt data as a function of |U| is shown for a five-attribute, three-owner, fixed-access policy. The calculation cost of the owner priority approach and the majority permit strategy are both greater than that of the complete permit strategy since the data owner must set up one or more empty policies for co-owners. It evaluates the data owner's communication expenses under three different scenarios. Overall, the amount of ciphertexts for all three methods grows linearly with Nc. Since the number of shares in C7, C8, C9, and C10 is doubled in the owner priority strategy compared to the full permit strategy, the communication cost of the majority permit strategy is the highest and the communication cost of the owner priority strategy is slightly more than the full permit strategy. Majority permit strategies have as many owners as there are permits available. In the phase of co-owner key generation, data co-owners establish access controls according to their privacy concerns and produce the transformation key using private keys. Given that three to five coowners of data are prevalent for scenarios in the real world, we analyse a common instance where the number of coowners is fixed to 5.

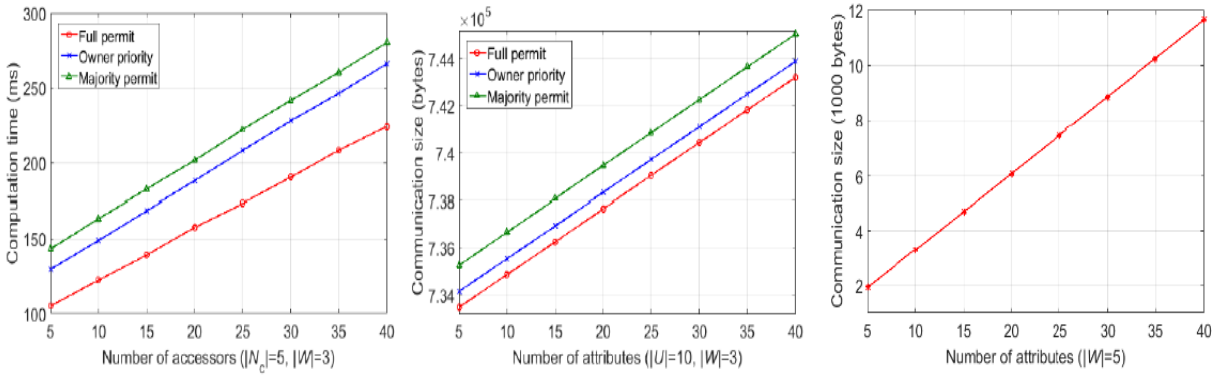

Fig.2 Comparative analysis of proposed system with existing system

V. FUTURE SCOPE AND CONCLUSION

Users worry about their data's privacy and security on the cloud. In particular, it becomes difficult to maintain data secrecy and address the privacy concerns of various owners. In this

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

study, we introduce a multi-owner, cloud-based, conditional sharing and dissemination method for sensitive data. Based on the IBBE method, our plan allows the data owner to encrypt sensitive information and then easily distribute it to several users simultaneously. Meanwhile, the data owner may use attribute-based CPRE to establish granular access policy to the cypher text, ensuring that it can only be re-encrypted by data disseminators whose characteristics meet the access policy in the cypher text. In addition, we provide a multiparty access control method over the cypher text that enables the data co-owners to append their access rules to the cypher text. To address the issue of privacy conflicts, we also provide three policy aggregation strategies: complete permit, owner priority, and majority permit. Eventually, we want to improve our approach by allowing for keyword search inside the encrypted message [47, 48].

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-collaborationand- 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/docu ment/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 on 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.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

[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.