IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9660

Multi-Owner Sharing Secure Data with Groups and Conditional Distribution using Cloud Computing

Karunakara [1], Dr. T Vijaya Kumar[2], Mr. Raghavendra Guligare[3]

Student, Department of MCA, Bangalore Institute of Technology, Bangalore, India[1]

HOD, Department of MCA, Bangalore Institute of Technology, Bangalore, India[2]

Project Manager, Weblitz Software, Bangalore, India[3]

Abstract: The fast improvement of Internet innovation and informal communities has brought about a high amount of remark texts being created on the Internet. In the period of large information, computerized reasoning advances can be utilized to mine the profound propensities of remarks for a more quickly information on network popular assessment. Feeling investigation is a computerized reasoning strategy, and its review is exceptionally valuable for deciding the opinion pattern of remarks. The message characterization task is at the core of opinion investigation, and different words contribute distinctively to arrangement. Most of contemporary feeling examination research utilizes dispersed word portrayal. Disseminated word portrayal, then again, exclusively examinations the semantic data of a word and overlooks the opinion data. The commitment of opinion data to the exemplary TF-IDF method is coordinated into this paper's proposed superior word portrayal approach, which creates weighted word vectors. The weighted word vectors are sent into BiLSTM (Bidirectional Long Short term Memory) to effectively gather setting data and better portray remark vectors. A feedforward brain network classifier is utilized to decide the opinion of the remark. The proposed feeling investigation approach is contrasted with RNN, CNN, LSTM, and NB opinion examination techniques under the indistinguishable circumstances.

Keywords:Cloud computing, project accreditation and secure data sharing

I. INTRODUCTION

Cloud computing is an internet-based computing method. Cloud computing will be used to share data the majority of the time. The cloud is a large region where you may access any type of data or information. On the basis of cloud computing, we all exchange data. Cloud computing facilitates the sharing of computer processing resources. In today's world, security is crucial. One of the major challenges in cloud computing is to provide additional security for data exchange. Encryption is a technique for securely transferring data between senders and receivers. This research presents a re-encryption mechanism for cloud computing to provide extra-large security. Any sort of data can be encrypted using a key. The key function generates a random key for the data source and the number of users. Based on the key mechanism, more security will be provided. The primary issue is hacked data from data sharing. Unauthorized users have access to data that hasn't been authenticated. As a result, the hacker has gained access to data. These issues are addressed in that study. The re-encryption approach is used in this research to give advanced security in cloud computing. The data must be stored above the Cloud Storage server. That server is known as the data provider, and the data provider is in charge of uploading data or files to the storage server. Using the key as well as the opt code, a large user can view the submitted data of files or download the files.

II. LITERATURE SURVEY

A number of unrecognised safety and protection concerns appear as major testing areas in distributed work out. the popularity of distributed computing stems from the benefits of large stockpiles of assets and instant access [1]. Effective encryption technologies should be used to maintain information secrecy in order to reduce these threats. A few strategies for sharing private information in distributed computing IBBE methodology were proposed by Liu et al. [9].In these designs, the owner of the information reacquires encoded data from the CSP by providing a list of beneficiaries; as a result, only the recipients of the list's may get the decoding keys and subsequently decrypt the secret data. For combining information encryption and granular access control in distributed computing, ABE is another another intriguing one-to-many cryptographic approach. categorise and protect information Access control methods must be put into place in order to guarantee secure information participation in distributed computing [4]. Cryptographic tools including character-based

(ABE) encryption [5, 6], personality-based broadcast (IBBE) encryption [7], and remote validation [8] have been utilised to solve these security and protection issues. To enable secure and precise information sharing in distributed computing, a unique cryptographic component called ABE is being deployed [8].

Maintaining the information dissemination system in various informal groupings in light of CP-ABE To attain security safeguarding in distributed storage frameworks, created an advantageous access control plot using progressive CP-ABE. When delivering health administrations in the cloud, ABE was used in the plans to provide access control of clinical reports; as a result, the wellbeing record must be decoded by authorised archive requesters with equivalent credits. Secure information dissemination is a crucial component of distributed computing's information capacity security need. Those who disseminate information could supply the semi-private section with their re-encryption keys intermediary to change the information proprietor's ciphertext for new clients with the help of the personality-based PRE , an important encryption calculation to achieve secure information dispersal in distributed computing.. Property-based PRE [17] has also been applied in distributed computing by merging the ABE method. In a democratic democracy, this concept suggests three methods for identifying multiparty protection disputes. Facebook's security paradigm may be exploited to offer multiparty protection, as demonstrated by Thomas et al. [20]. Xu et al. [19] developed a system that enables each client in an image to take part in choosing the access control states for the picture based on this multiparty security control paradigm.

IV. METHODOLOGY

A. System Model:

The associated molecules make up the framework model, as seen in Fig. 1. The documentation utilised for this investigation is summarised in Table 1.

1) Trusted Authority: The TPA provides public and generates private key as well as characteristic key for clients. It is a completely trusted component. For instance, a government retirement aid organisation or the association's director often carry it out.

2) Cloud Service Provider (CSP): For information co-owners, it additionally adds access strategies to the ciphertexts. provides consumers with re-encrypted ciphertexts.

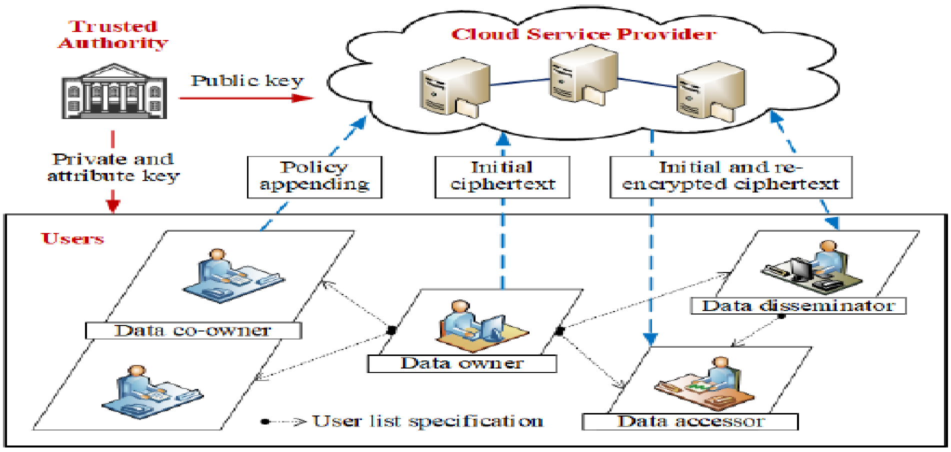


Fig. 1 shows the suggested scheme's system model. The categories of the user role are as follows: data owner, co-owner ,accessor and disseminator.

3) User: The trusted authority selects a bilinear map with the coordinates x->00:e T, where 0 and T are two's multiplicative groups with prime number x. Then, a trustworthy authority chooses at random a cryptographic hash function (x), a MAX number of receivers (N), and a security parameter (p). pH = 0 and 1, H = 20 and 0 and 1, TH = 3 and 0, and Tx = 4 and 0 H. The system then system public key is created along with the master secret key (,,)MK g.

γβ γ γγγ β β γβ γ =(, ,..., , , ,...., , , , , , , , (,), (,)) NN PK h hh u uu h h g g e g h (1).

DOI: 10.17148/IARJSET.2022.9660

B. Policy Aggregation Strategies

Data co-owners are able to renew the ciphertexts in our method by inserting their access regulations as the distribution condition. To meet the authorization requirements imposed by multi-owner, as shown in Fig. 2, we recommend the following tactics.
1) Full Permit: The right to determine the terms of data dissemination belongs to all owner, Owners of data are included and co-owners. The data disseminator is required to abide by any access guidelines set forth by that's owners.
2) Owner Priority: Despite the fact that owner tags the co-owners, the data owner's decision is final. The data cannot be distributed unless the data disseminator complies with all of the access requirements set out by the data owner or by any of the data co-owners.
3) Majority Permit: Data can only be distributed Whenever the sum of all access policies satisfying the disseminator characteristics is more than or equal to the threshold that was initially chosen by the data owner.

C. Data Confidentiality: A rigorous defence must be taken against unauthorised users and questionable CSPs. Users shouldn't have access to the plaintext unless the data owner or disseminator has specifically designated them as recipients of a ciphertext.

Fig. 2. Three multi-owner policy aggregation techniques

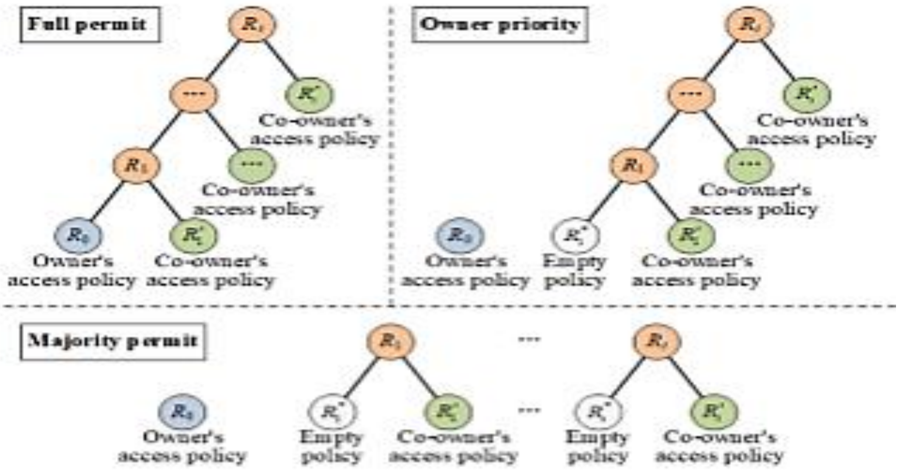
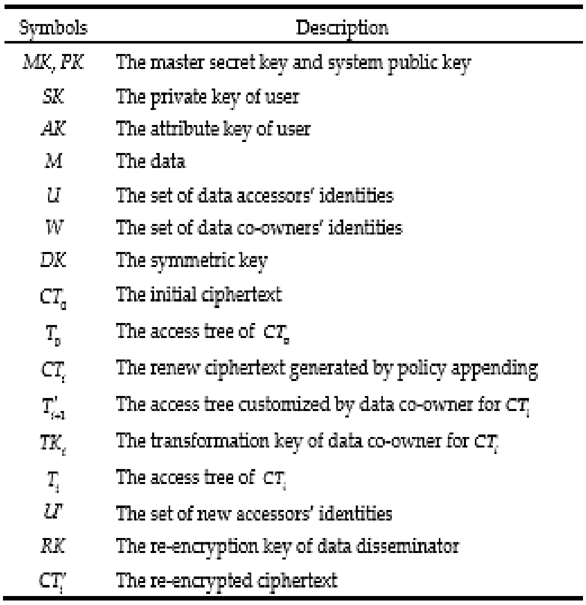


TABLE 1 Notations Symbol



Symbols	Description
MK, PK	The master secret key and system public key
SK	The private key of user
AK	The attribute key of user
M	The data
U	The set of data accessors' identities
W	The set of data co-owners' identities
DK	The symmetric key
CT_0	The initial ciphertext
T_0	The access tree of CT_0
CT_i	The renew ciphertext generated by policy appending
T'_{i+1}	The access tree customized by data co-owner for CT_i
TK_i	The transformation key of data co-owner for CT_i
T_i	The access tree of CT_i
U'	The set of new accessors' identities
RK	The re-encryption key of data disseminator
CT'_i	The re-encrypted ciphertext

DOI: 10.17148/IARJSET.2022.9660

V. IMPLEMENTATION

D. System Setup :

The trusted authority selects a bilinear map with the coordinates x->00:e T, where 0 and T are two's multiplicative groups with prime number x. Then, a trustworthy authority chooses at random a cryptographic hash function (x), a MAX number of receivers (N), and a security parameter (p). pH = 0 and 1, H = 20 and 0 and 1, TH = 3 and 0, and Tx = 4 and 0 H. The system then system public key is created along with the master secret key (,,)MK g.

γβ γ γγγ β β γβ γ =(, ,..., , , ,..., , , , , , , , (,), (,)) NN PK h hh u uu h h g g e g h (1).

E. Key Generation :

For the user with identification ID, the trusted authority creates the private key SK.

plus one one (()) H IDSK g (2) The attribute keys AK for the data distributor is generated by the trustworthy authority. For each attributes jS, A set of attributes is called S, it selects a random x and random r. The output of the AK looks like this.

γαβ α + ∈′= = = =() 02(,{ () , }) J J J J S AK H j D h D g D g (3)

F. Data Encryption :

The shard data should be represented by M. The data owner selects a set U of data accessor identities and a set W of data co-owner identities when || UNand || WN are both legitimate. The owner of the data then creates a policy based on a tree and selects a random DK to symmetrically encrypt data M using SE. The data owner selects a polynomial x p for each nodex in each access tree. The degree of the polynomial, x d, is set to 1 xx dk, which is one less than the criteria value, x k. These polynomials are chosen in descending order. The owner of the data chooses a secret at random to be the root node R, sets (0) Rp = secret, and then chooses R d otherpoints of R p at random to describe it completely. In order to fully define x p for any other nodex, it sets = () (0) (()) x parent x p, p index x and chooses x d extra points at random. The empty policy, in particular, only has one child and may be met by any data disseminator. The data owner then chooses ′,,, p kk at random, computing = b, and encrypts DK using the policy aggregation technique.

G. Securiity Analysis Defination :

The DBDH assumption states that no adversary with polynomial time capabilities can differentiate between the following two tuples: (,,, (,)) a b c abc g gg e g g and (,,, (,)) a b c r g gg e g g, where a, b, c, and r.

Theorem 1: According to the DBDH hypothesis, our method is secure from particular plaintext attacks. The selective identification and selected plaintext attack (INDsID-CPA) against the IBBE system in the random oracle model has failed [6]. Let C act as the challenger in the IND-sID-CPA security of the IBBE system. The security game we describe including challenger C, adversary A, and opponent B. In contrast to challenger C, who examines adversary B's capacity to compromise the IBBE scheme's security, opponent B serves as the adversary being tested by opponent A. Using the U* challenge IDs and T* challenge access policy, the adversary selects a set of U* challenge IDs. ,Let DBDH AAdv and IBBE AAdv represent the adversary's advantage in order to defeat the DBDH issue and the IBBE scheme, respectively. Assume adversary A completely queries the re-encryption key q times after playing the security game given in [36] and has the advantage of A Adv to defeat our method. In order to disable the IND-sID-CPA security of the IBBE scheme = IBBE DBDH IBBE (1) B A AA Adv Adv q Adv q Adv, Attacker B gets the upper hand. We know that IBBE BAdv and IBBE AAdv are irrelevant since the IBBE scheme is IND-sID-CPA safe in the random oracle model. The DBDH assumption is valid, hence the DBDH AAdv is likewise irrelevant as a result. Our technique is similarly IND-sID-CPA safe in the random oracle model since A Adv must be minimal. We then conduct an analysis to see whether our plan can adhere to the following security requirements for data exchange and dissemination in cloud computing

1) Information Privacy: Before being encrypted with a set of receiver identities and access limitations based on CP-ABE and IBBE, the cloud data is encrypted using a random symmetric key. As a result, people whose names are not included in the collection may be protected from accessing confidential material. Furthermore, the CSP is unable to get any sensitive data throughout any strategy's dissemination phase thanks to the secure CPRE technology.

DOI: 10.17148/IARJSET.2022.9660

2) Fine-Grained Data Dissemination: The attribute-based CPRE technique, which offers greater pliability in putting complex access requirements on data disseminators, further protects the symmetric key. The data owner and co-owners can design expressive and adaptable access restrictions to the ciphertext that permit AND and OR gates in accordance with their privacy preferences.

3) Collusion Resistance: The malicious data disseminators combining their strengths traits to propagate the ciphertext**.**

A. Functionality Comparisons:

Table 2 contrasts our system with a number of contemporary systems. Starting with the fact that the data owner and data co-owners may impose flexible fetchs controls above the ciphertexts, as opposed to who can only implement simple keyword requirements, our method is more advanced in fine-grained conditional distribution. In addition, even though Guo

VI. RESULTS

In this part, we put our technique into practise using the pairing-based cryptography library on A cloud server with a 2.53 GHz Intel Core 2 Duo processor and 4 GB of RAM. The 160-bit elliptic curve group and 512-bit finite field are based on the super-singular curve y2 = x3 + x, and the 80-bit security level and type are defined in the public parameters.

A number of tests are conducted before we select the Advanced Encryption Standard (AES) as the symmetric encryption method. The results of the Each experiment is based on 100 trials. During the encryption process, In addition, the data owner sets up an access policy and a set of identities, after which the encrypted data is uploaded to the CSP. Computed time and size of the communication are used to gauge complexity. The quantity of accessors and the characteristics of the access policy together account for the majority of the computation time. The calculation time of data encryption vs. |U| is shown in Figure 3 for the scenario of a fixed access policy with 5 characteristics and 3 co-owners. The calculation costs of the majority permit strategy and the owner priority strategy are higher than those of the entire permit strategy because, in each case, the data owner must set up one or more empty policies for co-owners. Figure 4 shows the communication expenses incurred by the data owner while using each of the three options. Overall, all three methods increase ciphertext sizes linearly with Nc. More specifically, the majority permit strategy's communication cost is the greatest, while the owner priority strategy's communication cost is somewhat higher than that of the full. The cost of communication at this period is shown in Figure 5. As illustrated in Fig. 6, we also calculate the price of introducing policies. The findings, in particular, demonstrate that, regardless of the method, the processing cost for each co-owner to impose their access policy on the ciphertext remains the same. The majority permit strategy produces the quickest results, which are practically constant at 0.18 milliseconds, and both the owner priority method and the entire permit strategy have about the same cost of policy appending. To examine whether the computation cost of re-encryption is linked to the number of features in the access policy, we set the number of attributes for each strategy . The calculation cost of re-encryption for each method is shown versus the number of features in Figure 7. If the threshold t is set to 1, and the calculation time is a little bit longer than in the owner priority strategy under access tree T0, the re-encryption will be successful if the data disseminator fulfils any of the access policies. The computation time on the accessor side vs the quantity of accessors when decrypting ciphertext is finally plotted in Fig. 8. Re-encrypted ciphertexts need far more time to decipher than original ciphertexts do. This is because, in order to decode the re-encrypted ciphertext, the data accessor must do one more pairing and hash operation. When there are 10 accessors and the ciphertext size is, the testing findings show that it takes around 122 milliseconds to apply the full permit strategy to encrypt the shared data.

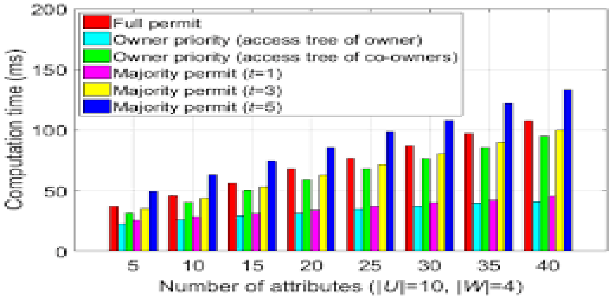


Figure 6 Computation cost of three strategies in policy appending phase.

DOI: 10.17148/IARJSET.2022.9660

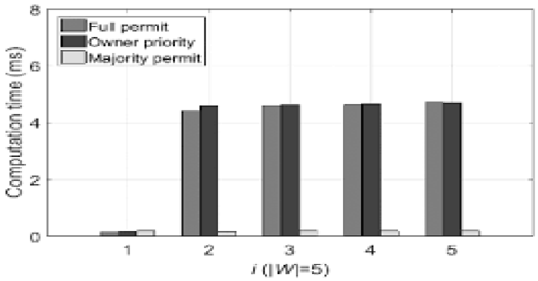


Figure 7 Computation cost versus attributes in re-encryption phase.

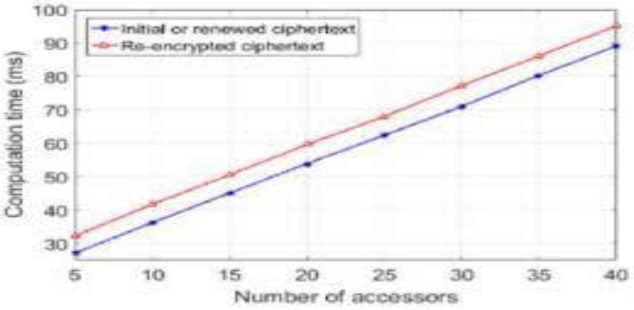


Figure 8 Computation cost versus accessors in decryption

VII. CONCLUSION

Data security and privacy are worries for cloud computing users. Enforcing many owners' privacy rights while upholding data confidentiality is particularly challenging. In this study, we provide a conditional dissemination and secure data group sharing method for cloud computing with many owners. According to the IBBE method, our solution allows the data to encrypt their personal information and simultaneously share it with a number of data accessors. As a result, re-encrypting the ciphertext is only allowed for data disseminators whose characteristics meet the access policy in the ciphertext. In the meanwhile, the data owner can use attribute-based CPRE to create granular access controls to the ciphertext. ACKNOWLEDGMENT Funding for this work was provided by the China Scholarship Council, the National Key Research and Development Program of China (2016YFB0800605), the Key Program of Joint Funds of the National Natural Science Foundation of China (U1736212), and the National Natural Science Foundation of China (61572080). (201806475007).

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.

DOI: 10.17148/IARJSET.2022.9660

[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/UnderstandingCollaborator-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.