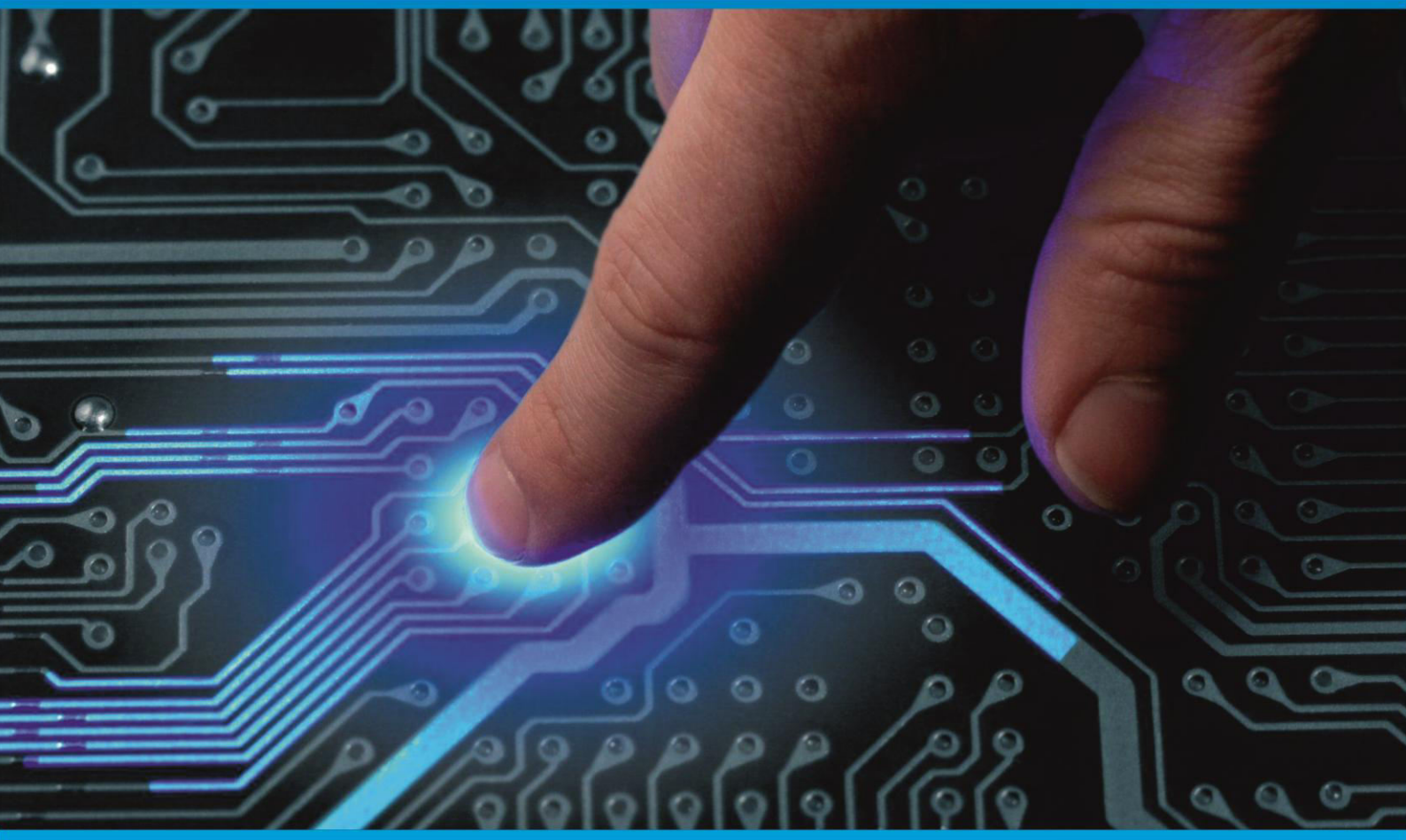
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

Signature Based Authentication in Cloud for Multi-Owner Data Sharing

Mohammadi Fatima[1], Maimuna Begum[1], Sadaf Naaz Farooqui[1], Hadiya Sameen[2]

B.E Students, Dept. of I.T., ISL Engineering College, Affiliated to Osmania University, Hyderabad, India[1]

Assistant Professor, Dept. of I.T, ISL Engineering College, Affiliated to Osmania University, Hyderabad, India[2]

ABSTRACT: With the quick improvement of cloud administrations, enormous volume of information is shared through distributed computing. Albeit cryptographic procedures have been used to give information classification in distributed computing, current instruments can't authorize security worries over ciphertext related with various proprietors, which makes co-proprietors incapable to fittingly control whether information disseminators can really scatter their information. In this paper, we propose a safe information bunch sharing and contingent scattering plan with multi-proprietor in distributed computing, in which information proprietor can impart private information to a gathering of clients through the cloud in a protected manner, and information disseminator can spread the information to another gathering of clients if the properties fulfill the entrance strategies in the code text. We further present a multiparty access control instrument over the scattered code text, in which the information co-proprietors can attach new access arrangements to the code text because of their security inclinations. In addition, three arrangement collection techniques, including full grant, proprietor need and lion's share license, are given to tackle the protection clashes issue brought about by various access strategies. The security investigation and test results show our plan is viable and productive for secure information offering to multi-proprietor in distributed computing.

KEYWORDS: Authentication, Data Owner, Multi Owner, Cloud Storage, Data Sharing

I. INTRODUCTION

The prominence of distributed computing is acquired from the advantages of rich stockpiling assets and moment access. It totals the assets of figuring framework, and afterward gives on-request benefits over the Internet. Numerous popular organizations are presently giving public cloud administrations, like Amazon, Google, Alibaba. These administrations permit singular clients and venture clients to transfer information (for example photographs, recordings and reports) to cloud specialist organization (CSP), to get to the information whenever anyplace and offering the information to other people. To ensure the protection of clients, most cloud administrations accomplish access control by keeping up access control list (ACL). Thusly, clients can decide to either distribute their information to anybody or award access rights only to their supported individuals. Be that as it may, the security hazards have brought worries up in individuals, because of the information is put away in plaintext structure by the CSP. When the information is presented on the CSP, it is out of the information proprietor's control. Lamentably, the CSP is generally a semi-confided in worker which sincerely follows the assigned convention, however may gather the clients' information and even use them for benefits without clients' assents. Then again, the information has enormous uses by different information purchasers to get familiar with the conduct of clients.

These security issues inspire the successful answers for ensure information privacy. It is fundamental to embrace access control components to accomplish secure information partaking in distributed computing. Presently, cryptographic components, for example, quality based encryption (ABE), character based transmission encryption (IBBE), and distant authentication has been abused to settle these security and protection issues. ABE is one of the new cryptographic instruments utilized in distributed computing to arrive at secure and fine-grained information sharing. It includes a system that empowers an entrance power over scrambled information utilizing access approaches and credited characteristics among decoding keys and cipher texts. However long the trait set fulfils the entrance strategy that the cipher text can be unscrambled. IBBE is another predominant strategy utilized in distributed computing, in which clients could impart their scrambled information to different collectors all at once and the public key of the beneficiary can be viewed as any legitimate strings, like extraordinary character and email. Truth be told, IBBE can be viewed as an exceptional instance of ABE for arrangements comprising of an OR door. Contrasted with ABE in which the mysterious key and cipher text are both compare to a bunch of characteristics, IBBE causes minimal expense key administration and little consistent approach sizes, which is more appropriate for safely communicating information to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

explicit recipients in distributed computing. Subsequently, by utilizing characters, information proprietor can impart information to a gathering of clients in a safe and effective way, which persuades more clients to share their private information through cloud.

As a matter of fact, these encryption strategies can forestall unapproved substances (for example semi-confided in CSP and vindictive clients) from getting to the information, however it may not consider information dispersal in distributed computing. In the cloud joint effort situation, for example, Box and OneDrive, the information disseminators (for example manager and teammate) may impart the reports to new clients even those external the association. Notwithstanding, when the information is scrambled with the above strategies, information disseminators can't adjust the ciphertext transferred by information proprietors. Intermediary re-encryption (PRE) plot is utilized to accomplish secure information spread in distributed computing by assigning a re-encryption key related with the new beneficiaries to the CSP. In any case, the information disseminator can disperse the entirety of the information proprietor's information to others with this re-encryption key, which may not meet the reasonable necessity since the information proprietor may just allow the information disseminator to spread a specific report. A refined idea alluded to as contingent PRE (CPRE) could resolve this issue, wherein information proprietor can implement re-encryption authority over the underlying ciphertexts and just the ciphertexts fulfilling explicit condition can be re-scrambled with comparing re-encryption key. Notwithstanding, customary CPRE conspires just help straightforward watchword conditions, so they can't coordinate with complex circumstances in distributed computing great. To help expressive conditions instead of catchphrases, property based CPRE is proposed, which conveys an entrance strategy in the ciphertext. The re-encryption key is related with a bunch of traits; in this manner the intermediary can re-encrypt the ciphertext just when the re-encryption key matches the entrance strategy. Thusly, information proprietor can modify fine-grained dispersal condition for the common information. For instance, information proprietor permits project chiefs in the association to spread the advancement report in OneDrive, while just allow leader chiefs in money office to scatter the venture financial plan in OneDrive during a particular time span.

II. RELATED WORK

A progression of unaddressed security and protection issues arise as significant exploration points in distributed computing. To manage these dangers, suitable encryption procedures ought to be used to ensure information privacy. By using the IBBE strategy, Huang et al., Patranabis et al. also, Liu et al. proposed a few private information sharing plans in distributed computing. In these plans, information proprietor re-appropriates encoded information to the CSP by characterizing a rundown of beneficiaries; subsequently just the proposed clients in the rundown can get the unscrambling key and further decode the private information. ABE is another promising one-to-numerous cryptographic procedure to acknowledge information encryption and fine-grained admittance control in distributed computing. Extraordinarily, ciphertext-strategy ABE (CP-ABE) is appropriate for access control in genuine applications because of its expressiveness in portraying the entrance strategy of ciphertext. Guo et al. proposed a protection safeguarding information scattering plan in versatile interpersonal organizations dependent on CP-ABE. Teng et al., proposed a productive access control plot with various leveled CP-ABE to accomplish protection safeguarding in distributed storage frameworks. In the plans of and, ABE has been used to give access control of clinical archives while giving wellbeing administrations in cloud, so wellbeing record must be decoded by approved report requesters with relating credits.

Secure information spread is another significant security prerequisite for information stockpiling in distributed computing. The character based PRE is a fundamental encryption calculation to reach gets information dispersal in distributed computing, with which the information disseminators could send their re-encryption keys to the semi-confided in intermediary to change information proprietor's ciphertext for new clients. Further, characteristic based PRE has been utilized in distributed computing by fusing the ABE method. The intermediary can change the ciphertext under an entrance strategy into the one under another entrance strategy with information disseminator's re-encryption key, and the clients who fulfill the new access strategy can get to the plaintext. In any case, the above PRE plans just permit information scattering in an all way. This issue is additionally tended to by CPRE plot, in which the intermediary can effectively re-encode the ciphertext just if the endorsed conditions are met. Nonetheless, in prior CPRE plans, the conditions are catchphrases just, which would restrict the adaptability while implementing complex designations in distributed computing. Yang et al. proposed a trait based CPRE conspire by sending an entrance strategy in a ciphertext produced by open key encryption. The re-encryption key is produced by the mysterious key related with a bunch of characteristics, which permits the intermediary to re-scramble the ciphertext just when these qualities fulfill the entrance strategy. Wang et al., proposed a pre-verification approach for sharing information in cloud, which accomplishes beneficiary's quality validation before the re-encryption activity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

The multiparty protection control among co-proprietors is fundamental in distributed computing. Thomas et al. showed how Facebook's protection model can be embraced to accomplish multiparty security. It permits all related gatherings to determine openness arrangements for the information, so clients can get to the information if fulfilling the openness strategies of proprietor and every one of the related gatherings. In view of this multiparty protection control model, Xu et al. planned a component to empower every client in a photograph to partake in the choice of access control states of the photograph. Nonetheless, the above plans may have security clashes issue, which don't consider how clients would really accomplish bargain. To determine the security clashes among multiparty (arranging clients), Such et al. proposed the primary computational instrument. The idea is to assess thing affectability, relative significance and readiness for each clashing arranging clients, and let the person who has less rigid security necessity bargain. Hu et al., proposed a precise way to deal with empower protection saving information imparting to multi-proprietor. This plan presents three techniques dependent on a democratic system to determine the multiparty security clashes. Shockingly, this plan just spotlights on co-proprietors' entrance power over plaintext information, and disregards the information classification towards semi-confided in CSP and malignant clients.

III. PROPOSED SYSTEM

A. *SYSTEM MODEL*

We propose a protected data pack sharing and unforeseen dispersal plot with multi-owner in circulated registering, in which data owner can give private data to a social event of customers through the cloud in a secured way, and data disseminator can dissipate the data to another get-together of customers if the qualities satisfy the passageway approaches in the cipher text. We further present a multiparty will control part over the dispersed ciphertext, in which the data co-owners can add new access ways to deal with the ciphertext due to their security tendencies.

1) Trusted authority: The trusted authority is a fully trusted part that initializes the system public key, and generates private keys as well as attribute keys for users. For example, it can be acted by the administrator of the organization or social security administration.

2) CSP: The CSP is a semi-trusted part that provides each user with a virtual space and convenient data storage service with the cloud infrastructure. It also appends access policies to the ciphertexts for data co-owners and generates re-encrypted ciphertexts for users.

3) User: We divide the user role into the following categories: data owner, data co-owner, data disseminator and data accessor. The data owner can choose a policy aggregation strategy and define an access policy to enforce Dissemination conditions. Then he encrypts data for a set of receivers, and outsources the ciphertext to CSP for Sharing and dissemination. The data co-owners tagged by data owner can append access policies to the encrypted data with CSP and generate the renewed ciphertext. The data disseminator can access the data and also generate the re-encryption key to disseminate data owner’s data to others if he satisfies enough access policies in the ciphertext. The data accessor can decrypt the initial, renewed and re-encrypted ciphertext with her or his private key.

B. SECURITY MODEL

In our scheme, data co-owners can renew the ciphertexts by appending their access policies as the dissemination conditions. As described, we provide following strategies to fulfil the authorization requirements from multi-owner,

1) Full permit: All owners (including data owner and data co-owners) have the same right to decide the dissemination conditions of data. The data disseminator should satisfy all the access policies defined by these owners.
2) Owner priority: The data owner’s decision has high priority, though he tags the co-owners. The data disseminator can disseminate the data only when he satisfies the access policy of data owner or all the access policies of data co-owners.
3) Majority permit: The data owner firstly chooses a threshold value, and the data can be disseminated if and only if the sum of access policies satisfied by disseminator’s attributes is greater than or equal to this fixed threshold.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

C. *DEFINITIONS AND NOTATIONS:*

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

D. *FUNCTIONALITY COMPARISON*

We first compare our scheme with several recent schemes, Firstly, our scheme is advanced in fine-grained conditional dissemination as data owner and co-owners could enforce flexible access policies on the ciphertexts, while data owner only can enforce simple keyword conditions achieved fine-grained conditional data dissemination based on ABE, it cannot support data group sharing which the basic requirement in cloud is computing. In our scheme, data disseminators can transform the encrypted data to a new group of users based on IBBE and attribute-based CPRE.

We also compare our scheme with Thomas et al, Such et al. and Hu et al., which are the latest multiparty access control schemes. Thomas et al., gives the definition and solution of multiparty access control, but it ignores the privacy conflicts which may happen when multiple users enforce their different privacy preferences on the shared data. Such et al. and Hu et al. solve the problem of privacy conflicts on plaintext based on concession evaluation mechanism and voting mechanism respectively, while our scheme supports multiparty access control on ciphertext and introduces three strategies of aggregating privacy references to solve the problem of privacy conflicts

FUNCTIONALITY COMPARISONS

Schemes	Data confidentiality	Multiple receivers	Secure dissemination	Re-encryption key generation	Conditional dissemination	Multiple access control	Privacy conflict
[29]	CP-ABE	Yes	Yes	-	Access policy	No	-
[36]	IBBE	Yes	Yes	Disseminator	Keyword	No	-
[40]	-	Yes	No	-	-	Yes	Concession evaluation
[41]	-	Yes	No	-	-	Yes	Voting
Our scheme	IBBE	Yes	Yes	Disseminator	Access policy	Yes	Policy aggregation strategies

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

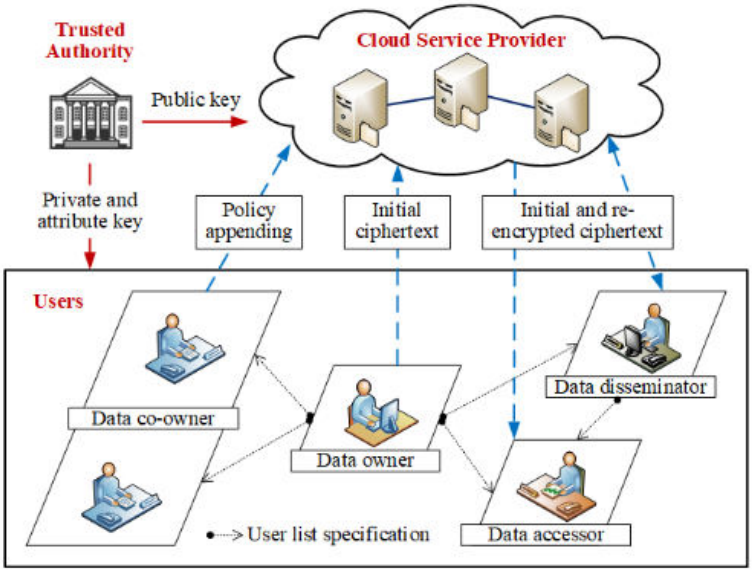
|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

E. PROPOSED SYSTEM ARCHITECTURE

We first assume that trusted authority is fully trusted by other entities and will not collude with any entities, which is also employed by related works. We then assume that CSP is semi-trusted, which will honestly execute the requests from the entities and may be curious to learn as much information about the stored data as possible. Besides, we assume that data owners are trusted, but some users will try to access the data beyond their privileges, even by colluding with other users and CSP. Further, we do not consider data version management, which means once a ciphertext is renewed, the users cannot obtain the previous ciphertext, and we assume that the ownership of data can be guaranteed by the ciphertext deduplication scheme. Specifically, the security goals are summarized as follows.

1) Data confidentiality: The data should be well protected against the semi-trusted CSP and unauthorized users. The users who are not the receivers of a ciphertext defined by the data owner or data disseminator should not be able to access the plaintext.
2) Fine-grained dissemination conditions: The data owner and data co-owners can customize fine-grained and tree-based dissemination conditions for their data. The ciphertext can only be disseminated by the users who satisfy these conditions.
3) Continuous policy enforcement: The data owner's access policy is enforced in the initial ciphertext as well as the renewed ciphertext.
4) Collusion resistance: If each of the data disseminators' attributes cannot satisfy the access policies in the ciphertext individually with their own attributes, these users could not collude and decrypt this ciphertext.



System model of proposed scheme

The user role is divided into the following categories: data owner, data co-owner, data disseminator and data accessor.

IV. RESULTS

Our experiments and chooses the Advanced Encryption Standard (AES) as the symmetric encryption scheme. The experimental results are the mean of 100 trials. In the encryption phase, data owner defines a set of identities and an access policy, and then uploads the encrypted data to the CSP. We utilize the computation time and communication size as the metric to measure complexity. The computation time is mainly related to two factors, that are number of accessors and attributes in the access policy.

Fig. 3 shows the computation time of data encryption versus |U| under a fixed access policy with 5 attributes and 3 co-owners. Due to data owner should set up one and multiple empty policies for co-owners in owner priority strategy

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

and majority permit strategy respectively, the computation cost of these two strategies is higher than that of full permit strategy.

Fig. 4 compares the communication cost of data owner when he chooses each of three strategies. On the whole, ciphertext sizes in three strategies are all increasing linearly with N. More particularly, communication cost of majority permit strategy is the highest, and the communication cost of owner priority strategy is a little more than full permit strategy, since the number of shares of C, C8, C9, and C in owner priority strategy is twice as much as that in full permit strategy. The number of shares in majority permit strategy is equal to the number of co-ownersIn the co-owner key generation phase, the data co-owners define access policies according to their privacy concerns and generate the transformation key with private keys. We consider a common case where the number of co-owners is fixed to be 5, since three to five data co-owners are very common for situations in real world. The communication cost in this phase is given in

Fig. 5We also measure the computation cost of policy appending, as shown in. In particular, the results show that the computation cost of each co-owner in each strategy to enforce her or his access policy on the ciphertext. It can be observed that the cost for policy appending is almost the same in full permit strategy and owner priority strategy, and the result in majority permit strategy is the lowest and almost constant in 0.18 ms.

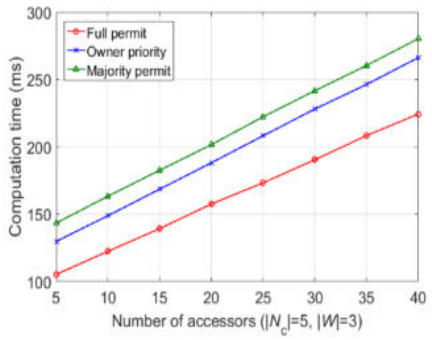


Fig. 3. Computation time versus users in encryption phase.

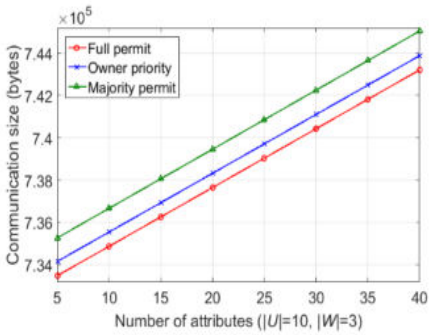


Fig. 4. Communication size versus attributes in encryption phase.

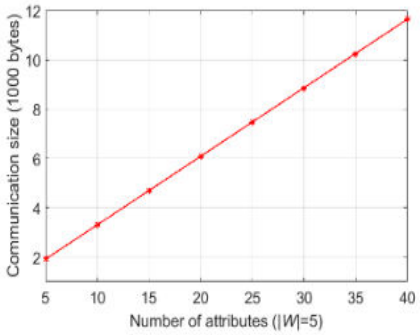


Fig. 5. Communication size versus attributes in co-owner key generation phase.

V. CONCLUSION AND FUTURE WORK

The information security and protection is a worry for clients in distributed computing. Specifically, how to uphold security worries of different proprietors and ensure the information classification turns into a test. In this paper, we present a safe information bunch sharing and contingent spread plan with multi-proprietor in distributed computing. In our plan, the information proprietor could encode her or his private information and offer it with a gathering of information accessors at one time in a helpful manner dependent on IBBE procedure. In the meantime, the information proprietor can indicate fine-grained admittance strategy to the ciphertext dependent on characteristic based CPRE; subsequently the ciphertext must be re-scrambled by information disseminator whose credits 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 annex their entrance strategies to the ciphertext. Additionally, we give three strategy conglomeration techniques including full grant, proprietor need and dominant part license to take care of the issue of security clashes. Later on, we will improve our plan by supporting catchphrase search over the ciphertext.

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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905169 |

[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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details