

Secure Data Sharing with Multiparty Access Control on Cloud

Sangeetha.S¹, Prasanth.K² and Rohan.N³

¹Assistant Professor, Department of Information Technology, Kongunadu College of Engineering and Technology, Trichy, India

Email: sangiacademics@gmail.com

²⁻³Final year, Department of Information Technology, Kongunadu College of Engineering and Technology, Trichy, India

Email: {rohanrohit9274, prasanthkongu4}@gmail.com

Abstract—Access control is a general a policy or procedure that allows, denies or restricts access to a system. It may monitor and record all attempts made to access a system. Access Control identifies users attempting to access a system unauthorized. It is a mechanism which is very important for protection in computer security. Various access control models are in use, including Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All the models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in distributed system, where there are only a set of Users with known set of services. In these systems, users and resource providers are not in the same security domain. Mostly Users are normally identified by their attributes or characteristics and not by predefined identities. Hence, the access control Mechanism must be flexible to support various kinds of domains and policies, etc. With the development of large distributed systems attribute based access control (ABAC) that will show the as more as become very increasingly slightly is one of the important.

Index Terms— Access control, Mandatory Access Control (MAC), Role Based Access Control (RBAC), Attribute based access control (ABAC).

I. INTRODUCTION

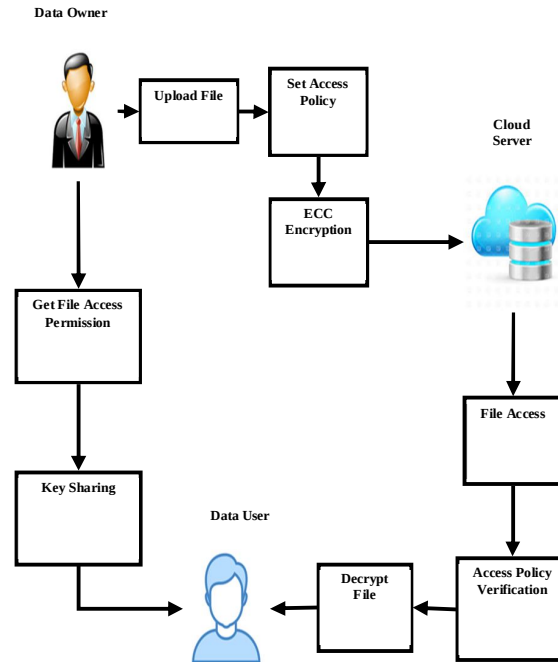
The first way a system provides security to its resources and data, is by controlling access to the resources and the system itself. However, access control is more than just controlling which users (subjects) can access which computing and network resources. In addition, access control manages users, files and other resources. It controls user's privileges to files or resources (objects). In access control systems various steps like, identification, authentication, authorization and accountability are taken before actually accessing the resources or the object in general. In early stages of computing and information technology, researchers and technologists realized the importance of preventing users from interfering each other on shared systems. Various access control models were developed. User's identity was the main index to allow users to use the system or its resources.

However, with the growth of the networks and the number of users, IBAC was found to be weak to defend such a large growth. Advanced concepts in access control were introduced which included owner/ group/ public. IBAC proved to be problematic for distributed systems as well. Managing access to the system and resources became hard and vulnerable to errors. A new method known as Role Based Access Control (RBAC).

II. SYSTEM DESIGN

An attribute-based scheme was proposed for verifiable keyword search on outsourced encrypted data, which allows data owners to control the search permission according to an access control policy for the encrypted data, and allow data owners to verify the correctness of search. Although their scheme is in multiuser settings, it supports a single-keyword search. Attribute encryption allows the sender to encrypt the message without obtaining the public key certificate. An ability to encrypt data with a public key without certificates in some cases is a solution of the problem.

For example, the user **A** can send an encrypted message to the recipient **B** without PKI or when the recipient is not connected at the time of transmission. Personality is viewed as a set of many descriptive attributes using attribute-based encryption. A user with a secret key ω can decrypt data encrypted with the public key ω' , if and only if ω and ω' differ slightly. The threshold of insignificance of differences is set by some metric d assuming the sender wants to encrypt the document for all users who have a specific set of attributes. For example, the head of the bus fleet wants to convey information in an encrypted form to drivers. In this case, the data is encrypted with the attribute of the form: {"bus fleet", "Head", "driver"}.



III. RESULT AND ANALYSIS

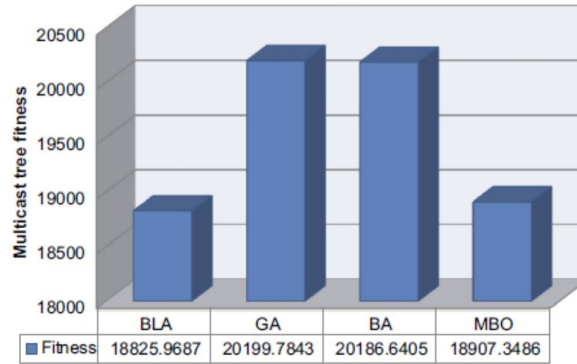
To demonstrate the performance of BLA compared to the other algorithms (GA, BA and MBO), the average rounded values of ten (10) best fitness obtained in each test for different algorithms are calculated and listed in Table 3. From Table 4.1 and Fig. 9, we mark that the best fitness is the fitness obtained by BLA (18,825.9687). It is better than other.

To compare the complexity of BLA in contrast with other approaches (GA, BA and MBO), we summarize time computing in Fig. 11 and Table 4. This figure illustrates the inactivity of the best solution fitness for each population with time consumed by each algorithm. One can note that BLA algorithm reached the best fitness (18,825.96) in the earliest generation (13th generation). This proved its low time complexity compared to the others approaches. For example, MBO algorithm reached its stagnation state at the 16th generation. We note that the stagnation generation of BA algorithm is obtained at the 7th generation but with bad value (20,186.64).

Best results given by BLA, GA, BA and MBO in terms of cost, delay, jitter and bandwidth.

	BLA	GA	BA	MBO
Fitness	18,825.9687	20,199,7843	20,186,6405	18,907,3486
Cost	1,732.386	1,869,8364	1,868,534	1754,657
Delay	617,011	616,249	616,134	493,149
Jitter	8,75487	8,75343	8,75165	7,00506
Banwidth	797,549	797,637	797,65	797,579

In this case, BA dropped in a local optima value in an early time. Moreover, GA stagnated in the 16th generation. This practical analysis showed that BLA converge to the optimal solution better than GA, BA or MBO with the least generation times. They confirm reliability and efficiency of BLA to solve the QoS-MRP with a minimum time compared to other approaches. In fact, performances of BLA are due to the generalization of the proposed algorithm in terms of the optimization principles. It collects global search using the crossover operator which guarantees the diversity of the solution. Also, it ensures the local optima escape. Furthermore, BLA carries out local search in the mutation operator and also in the neighbor-hood search approach.



IV. CONCLUSION

Data security is a major problem to be dealt with from a few decades. In this paper we have reasoned the use of cryptographic techniques for securing the data. Here discussed about data security algorithms with ECC. These algorithms help in securing in transit data. Thus ECC is the cryptographic algorithm which provides security and authentication. The RBAC system can possibly be valuable in commercial situations as it captures practical access policies based on roles in an adaptable way and gives secure data storage in the cloud upholding these access strategies and the ABAC plan can empower the data owner to appoint a large portion of computation overhead to capable cloud servers. Confidentiality of user access to benefit and user secret key responsibility can be accomplished. Formal security proofs demonstrate that this plan is secure under standard cryptographic models.

FUTURE ENHANCEMENT

Provide a highly efficient model for provide combined access control mechanism in cloud computing. It is in a hierarchical structure and it using server and owner combined access control model. This model ensure both security and access control in cloud computing.

REFERENCES

- [1] Li, Jin, Xiaofeng Chen, Jingwei Li, ChunfuJia, Jianfeng Ma, and Wenjing Lou. "Fine-grained access control system based on outsourced attribute-based encryption." In European Symposium on Research in Computer Security, pp. 592-609. Springer, Berlin, Heidelberg, 2011.
- [2] Chu, Cheng-Kang, Wen-Tao Zhu, Jin Han, Joseph K. Liu, JiaXu, and Jianying Zhou. "Security concerns in popular cloud storage services." IEEE Pervasive Computing 12, no. 4 (2011): 50-57.

- [3] Jiang, Tao, Xiaofeng Chen, Jin Li, Duncan S. Wong, Jianfeng Ma, and Joseph Liu. "TIMER: Secure and reliable cloud storage against data reoutsourcing." In International Conference on Information Security Practice and Experience, pp. 346-358. Springer, Cham,
- [4] Akinyele, Joseph A., Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin. "Charm: a framework for rapidly prototyping cryptosystems." *Journal of Cryptographic Engineering* 3, no. 2 (2014): 111-128.
- [5] Li, Jin, Xiaofeng Chen, Jingwei Li, ChunfuJia, Jianfeng Ma, and Wenjing Lou. "Fine-grained access control system based on outsourced attribute-based encryption." In European Symposium on Research in Computer Security, pp. 592-609. Springer, Berlin, Heidelberg, 2015.
- [6] Liang, Kaitai, Liming Fang, Willy Susilo, and Duncan S. Wong. "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security." In Intelligent Networking and Collaborative Systems (INCoS), 2015 5th International Conference on, pp. 552-559. IEEE, 2015.