IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 8, August 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 8, August 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1108024 |

Secure and Verifiable Policy Update Outsourcing for Bigdata Access Control in the Cloud

[1]Dr. T. GEETHA , [2] D. PRABHAKARAN, [3]R.PREETHI

Head, Department of MCA, Gnanamani College of Technology, Namakkal, India[1]

Assistant Professor, Department of MCA, Gnanamani College of Technology, Namakkal, India[2]

Student, Department of MCA, Gnanamani College of Technology, Namakkal, India[3]

ABSTRACT: Due to the high volume and velocity of big data, it is an effective option to store big data in the cloud, as the cloud has capabilities of storing big data and processing high volume of user access requests. Attribute-Based Encryption (ABE) is a promising technique to ensure the end-to-end security of big data in the cloud. However, the policy updating has always been a challenging issue when ABE is used to construct access control schemes. A trivial implementation is to let data owners retrieve the data and re-encrypt it under the new access policy, and then send it back to the cloud. This method, however, incurs a high communication overhead and heavy computation burden on data owners. In this paper, we propose a novel scheme that enabling efficient access control with dynamic policy updating for big data in the cloud.

We focus on developing an outsourced policy updating method for ABE systems. Our method can avoid the transmission of encrypted data and minimize the computation work of data owners, by making use of the previously encrypted data with old access policies. Moreover, we also propose policy updating algorithms for different types of access policies. Finally, we propose an efficient and secure method that allows data owner to check whether the cloud server has updated the cipher texts correctly. The analysis shows that our policy updating outsourcing scheme is correct, complete, secure and efficient.

KEYWORDS: Attribute-Based Encryption, re-encrypt, implementation, encrypted data.

I. INTRODUCTION

For some electronic devices, which are composed of dedicated hardware equipment, i.e., field programmable gate array (FPGA), digital signal processor (DSP) and integrated circuit (IC), the compatibilities for different requested tasks are difficult to guarantee and the systems will be more complicated with the increase in the number of the requested tasks. The software defined network (SDN) and virtualization technology are the foundations of the cloud computing, and provide a promising and flexible approach to facilitate resource allocation.

Cloud Service providers can allocate the available resources related to service nodes to the requested tasks depending on demand and supply. When a task consists of multiple subtasks, these sub-tasks could be deployed on several service nodes and form a service chain, which is a data flow through the service nodes in sequence and can be presented as a directed acyclic graph (DAG). Each sub-task needs the physical resources for central processing unit (CPU), memory, or graphic processing unit (GPU).

Besides, there are bandwidth costs to transfer data on different service nodes. For example, in case of data transmission, it includes five sub-tasks and the service chain about these sub-tasks can be represented as: network receiving capture - tracking - synchronization - decoding, where each functional module is achieved by software programming and can run on a commonly used computer system.

The complexity and development cost of a system can be effectively reduced by cloud computing, and the flexibility and scalability can also be improved. However, a new challenge in cloud computing is how to effectively allocate the available resources related to service nodes to the requested tasks, which leads to a combinatorial optimization problem.

II. EXISTING SYSTEM

However, as the scale of the optimization problem grows, a large feasible solution space needs to be searched and the computational complexity order of seeking the optimal solution increases. In the next section, we propose the HMAO algorithm, which is an optimization approach using hierarchical multiagent framework, to address the resource allocation problem in cloud computing.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 8, August 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1108024 |

DISADVANTAGES

- However, as the scale of the optimization problem grows, a large feasible solution space needs to be searched and the computational complexity order of seeking the optimal solution increases.
- The optimization problems for resource allocation in cloud computing have been widely studied

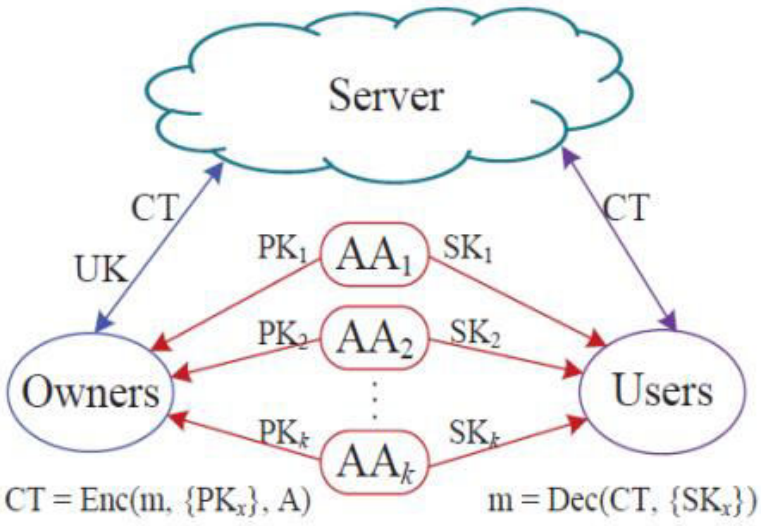
PROPOSED SYSTEM

In our work, a hierarchical multi-agent optimization (HMAO) algorithm is proposed to address the problem of maximizing the resource utilization and making the bandwidth cost minimum. The proposed HMAO algorithm consists of improved GA and multi-agent optimization (MAO) algorithm. For the MAO algorithm, we design a shared agent and several service agents. Shared agent can hold the information about resource allocation and task deployment for all service nodes.

ADVANTAGES

- Compared with centralized optimization methods, distributed optimization algorithms based on multi-agent systems (MAS) have an explicit potential advantage for solving the task deployment and resource allocation in cloud computing.
- Aim is to migrate and swap these sub-tasks on different service agents to reduce their bandwidth costs.

III. SYSTEM ARCHITECTURE



MODULE

- Cloud Module
- Group Manager Module
- Group Member Module
- File Security Module
- Group Signature Module
- User Revocation Module

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 8, August 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1108024 |

MODULE DESCRIPTION

CLOUD MODULE

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

GROUP MANAGER MODULE

Group manager takes charge of followings,

- System parameters generation,
- User registration,
- User revocation, and
- Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

GROUP MEMBER MODULE

Group members are a set of registered users that will

- Store their private data into the cloud server and
- Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

FILE SECURITY MODULE

- Encrypting the data file.
- File stored in the cloud can be deleted by either the group manager or the data owner. (i.e., the member who uploaded the file into the server).

GROUP SIGNATURE MODULE

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

USER REVOCATION MODULE

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 8, August 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1108024 |

IV. RESULT

V. CONCLUSION

To maximize the resource utilization based on CPU, memory and GPU, and minimize the bandwidth cost. To address the problem, propose the HMAO algorithm which combines the improved GA and the MAO algorithm, where the improved GA is to find an optimal resource utilization solution and the MAO algorithm is to minimize the bandwidth cost. For the MAO algorithm, use a priority-based selection mechanism to obtain the candidate source sub-tasks, and design the selection and exchange operators by a probabilistic method to migrate and swap the sub-tasks on several service agents. The proposed HMAO algorithm can obtain the objective optimal result by cooperative co-evolutionary method.

VI. FUTURE ENHANCEMENT

A hierarchical matching algorithm for service selection and resource purchasing in wireless network virtualization. Distributed implementation of the proposed algorithm has also been discussed in detail. Numerical studies have shown that the proposed hierarchical matching algorithm converges in a reasonable amount of time. Moreover it outperforms the fixed sharing algorithm and achieves comparable performance to a general sharing approach in terms of average sum-rate. As a future extension, we intend to include dynamic pricing and study its impact on the system's performance.

REFERENCES

1. H. Kim and N. Feamster, "Improving network management with software defined networking," IEEE Commun. Mag., vol. 51, no. 2, pp. 114–119, Feb. 2013.
2. S. Sezer et al., "Are we ready for SDN? Implementation challenges for software-defined networks," IEEE Commun. Mag., vol. 51, no. 7, pp. 36–43, Jul. 2013.
3. H. Erdogmus, "Cloud computing: Does Nirvana hide behind the Nebula?" IEEE Softw., vol. 26, no. 2, pp. 4–6, Mar./Apr. 2009.
4. H. Moens and F. De Turck, "VNF-P: A model for efficient placement of virtualized network functions," in Proc. 10th Int. Conf. Netw. Service Manage., 2014, pp. 418–423.
5. S. M. A. Kazmi, N. H. Tran, T. M. Ho, and C. S. Hong, "Hierarchical matching game for service selection and resource purchasing in wireless network virtualization," IEEE Commun. Lett., vol. 22, no. 1, pp. 121–124, Jan. 2018.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 8, August 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1108024 |

6. H. Zheng, Y. Feng, and J. Tan, "A hybrid energy-aware resource allocation approach in cloud manufacturing environment," IEEE Access, vol. 5, pp. 12 648–12 656, 2017.
7. L. Qu, C. Assi, and K. Shaban, "Delay-aware scheduling and resource optimization with network function virtualization," IEEE Trans. Commun., vol. 64, no. 9, pp. 3746–3758, Sep. 2016.
8. B. Muthulakshmi and K. Somasundaram, "A hybrid ABC-SA based optimized scheduling and resource allocation for cloud environment," Cluster Comput., vol. 22, pp. 10769–10777, 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

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