International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 8 ǁ 2021 ǁ PP. 87-90

Analysis of Data Access Control Methods to Ensure Security for The Cloud Storage

Kavyasri M N
Assistant Professor, Dept. of Computer Science & Engineering
Malnad College of Engineering Hassan

Abstract— *cloud storage is an important development trend in information technology data access control is an effective method to insure data security in cloud storage services. There are various data access control methods proposed to ensure security for the cloud storage based on encryption techniques, for datasets stored in an untrusted cloud environment, access control to enable an application to dynamically adapt to ngrowing workloads by increasing the number of servers. In this paper analysis of various access control methods are done based on the objectives methodologies applied and results of the work*

Keywords*-Cloud storage, access control; Attribute encryptionalgorithm; block chain; key value DB*

Date of Submission: 12-08-2021 Date of acceptance: 27-08-2021

I. INTRODUCTION

With the popularization and application of cloud computing technology, people have the ability to use large-scale distributed computing resources in the network. Cloud computing as a hot topic of research and application in recent years, most IT companies and industry insiders believe that the next generation of computer network application technology core architecture. Under the cloud computing environment, users do not have to spend the high cost of hardware and software to powerful computing resources and huge storage capacity, all of which can be handed over to the cloud computing service providers to complete. Not only saves the cost, but also does not need to expend the massive energy.The threat of network security is increasing, the network has a strong dependence on cloud computing is inevitable in the application process there are many security risks. In the traditional IT service solution, the vast majority of application software and data information is running or stored in the user's local physical equipment, in the user's absolute controllable range

A lot of users store their documents in clouds. Nevertheless, there are some security problems and copyright aspect. The essential problem is transferring data to the external environment, such that anyone else other than the owner can get access to information. On the other hand, it is difficult to give in to the numerous facilities that provide services for data storage: backup files, the ability to access their documents from any device from anywhere in the world, easy transfer of files to other users. we can find several ways to solve the problem of secure remote file storage. data access control is an effective method to insure data security in cloud storage services. There are various data access control methods proposed to ensure security for the cloud storage based on encryption techniques, for datasets stored in an untrusted cloud environment, access control to enable an application to dynamically adapt tongrowing workloads by increasing the number of servers.

II. ACCESS CONTROL SCHEMES

A. Fine-grained Access Control Scheme Based on Cloud Storage

This paper researched on security problem based on encryption, and proposed

scheme according to system characteristics of data storage on cloud platform, and applied it in cloud storage system with fine-grained access control based on CP-ABE.it came up with the experimental results proposed scheme optimized the user revocation, reduced the time of data owner to manage data, and realized the safe sharing and efficient storage of sensitive data in the public cloud storage.

Advantages:

A secure and efficient cloud storage system with an access control system based on CP-ABE it is a high efficient storage scheme based on data sharing and secret sharing, while only keeping a copy of the data. This scheme can significantly reduce the workload of DO and the storage space overhead of CSP, which can effectively promote the use of cryptography in the cloud storage system. At the same time, the security analysis proves that the system is safe. From the theoretical analysis and the actual test results, it can be seen that SECSS in the user revocation and storage space overhead is more efficient than OSCSS. Therefore, in the case where frequent and large amount of data is revoked, CSP and DO will benefit from that.

B. AYA: "an efficient access-controlled storage and Processing for cloud-based sensed data".

This paper proposed a new security architecture that Reinforces access-controlled data ownership on outsourced service from public c10ud environment. Specifically our solution is based on the design of an optimized implementation of Cp - ABE algorithm for enhancing privacy. In addition it allows secure and efficient data owner access-controlled by using Attribute-Based encryption (ABE) in the perspective of a paring-based Cryptosystem (PBC) and Iightweight token based authentication algorithm (using ECDSA) for the effectiveness of our solution in terms of computation and storage cost.

This scheme is proved to be semantically secured and efficient in terms of communications and computations costs. This scheme ensures the data owner to have control over his data access and delegates securely the heaviest part of computation to the trusted point (TP) and private cloud, which in this scheme serve as proxy between data owner and public cloud.

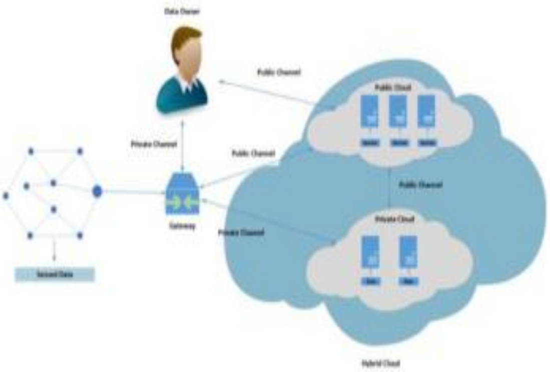

Figure: AYA model

C. An IO optimized Data Access Method in Distributed KEY-VALUE Storage System.

Distributed KEY-VALUE storage system is a new storage framework in cloud computing. It can enable an application to dynamically adapt to growing workloads by increasing the number of servers. current distributed KEY-VALUE storage systems are still inefficient on range query for larger of the result set. When the result set become large, the file layout, cache hit rate are both key points for IO efficiency. work showed the experience under the development of China Mobile Big Cloud KEY-VLAUE DB (BC-kvDB)., how to increase IO efficiency in BC-kvDB. BC-kvDB is based on single-table space data model and provides SQL-LIKE DDL and DML language. BC-kvDB's high throughput is a benefit of data locality storage, column-storage structure and multilayer caches. Data can be accessed through block index in local cache or local blocks. Experimental results show that the BC-kvD random writing performance ois 2.5 times better than HBase and the random reading performance is 1.8-2 times than HBase.

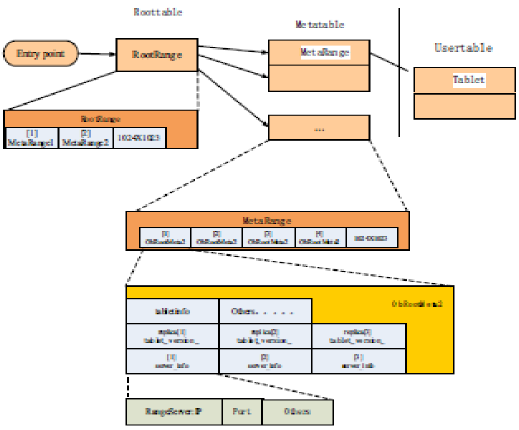

Figure: metatable structure of BC-kvDB

This work describes a high-performance distributed KEY-VALUE storage system (BCkvDB) and the data access method. In BC-kvDB the key-value pairs are compressed into blocks and indexed in a local data file. The region server can retrieve local data file directly for the range query. This can boost the query process for larger data set greatly. Besides, the cell cache, block cache and the shadow cache make the results are mostly hit in the local cache. The multi-layered cache can further increase the query efficiency.

D. A Blockchain-Based Access Control System for Cloud Storage

Above work proposed a prototype of multi-user system for access control to datasets stored in an untrusted cloud environment. Cloud storage like any other untrusted environment is in need of the ability to secure share information. It provides an access control over the data stored in the cloud without the provider participation. The main tool of access control mechanism is ciphertext-policy attribute-based encryption scheme with dynamic attributes. Using a blockchainbased decentralized ledger, it provides immutable log of all meaningful security events, such as key generation, access policy assignment, change or revocation, access request. It Proposed a set of cryptographic protocols ensuring privacy of cryptographic operations requiring secret or private keys. Only hash codes of ciphertexts are transferred through the blockchain ledger.

The main result of this work is the implementation of a software system prototype that implements the access control model of the system to data stored in untrusted environments.
To implement the system algorithms have been selected acceptable complexity, functionality, and complexity of implementation.

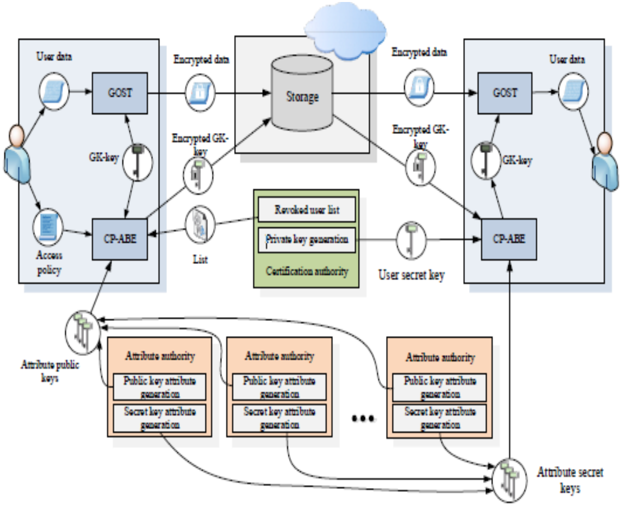

Figure: ABE scheme to access control in cloud storage

Key benefits of access control system are: the ability to customize the access policy for the encrypted data without duplicating them to a large number of participants; the ability to define dynamic access policies; access policy change does not require any additional action from other members of the

system, which avoids the need for regular changes to user keys; the integrity of information about all transactions, including the granting and changing access, facts gain access to file, rejection of the fact and the inability to edit these data is guaranteed through the use of the blockchain and smart contracts.

TABLE I. ANALYSIS OF ACCESS CONTROL METHODS

Access method	***Methodologies***	***Objective***	***Results***
Fine-grained Access Control Scheme Based on Cloud Storage	System storage on cloud platform, Cp-ABE algorithm, based on data sharing and secret sharing	Main focus on opoimization, to make an optimal balance between the system security and the overall overhead	reduce the workload of DO and the storage space overhead of CSP, security analysis proves that the system is safe
An IO optimized Data Access Method in Distributed KEY-VALUE Storage Syste	BC-kvdb	To increase data access rate for growing workloads by increasing the number of servers	Multilayered cache can increase query efficiency
Aya: "n efficient access-controlled storage and Processing for cloud-based sensed data"	Optimized implementation of cp-abe algorithm, attributed based encryption scheme	Access control of outsourced data ,data integration and privacy protection	Efficient in communication and computation costs
A Blockchain-Based Access Control System for Cloud Storage	Cipher text policy, Attributed based encryption scheme	Access control of data in the cloud without the provider participation	customize the access policy for the encrypted data without duplicating them to a large number of participants, dynamic access policies

III. CONCLUSION

With concern of data security many organizations are worried. Our main aim is to provide security during access of data. Various methods were proposed based on various techniques like those being explained in the paper . analysis of those methods are done and the results are given in the table For ensuring safety there is need to promote secure access of data at the data centers of cloud, optimization in data access with less encryption time and key generation time isrequired and there is also need of efficient attribute revocation.

REFERENCES

[1]. S. S. Muthukumaran and T. Ramkumar “An Approach forEnhancing Secure Cloud Storage Using Vertical Partitioning Algorithm”, Middle-East

[2]. N. N. Pathak , M. Nagori “Enhanced security for multi cloud storage usingnAES algorithm”, International Journal of Computer Science and Information Technologies, vol. 6 , pp. 5313-5315, 2015. Journal of Scientific Research, vol.23,no. 2, pp. 223-230, 2015.z

[3]. Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and Privacy Challenges in Cloud Computing Environments." IEEE Security & Privacy 8.6 (2010): pp. 24-31.

[4]. Xiaojie Niu. “Fine Grained access control scheme based on cloud storage, international conference on computer network, Electronic and Automation

[5]. AYA: an efficient access controlled storage and processing for cloud based sensed data

[6]. Wang, F., Chang, C.-C., Harn, L., “Simulatable and secure certificate-based threshold signature without pairings,” Security and Communication Networks, 2013, 7, (11), pp. 20942103.

[7]. Fournaris, A.P., “A distributed approach of a threshold certificate-based encryption scheme with no trusted entities,” Inf. Secure. J. Glob. Perspect., 2013, 22, (3), pp. 126139

[8]. Kate, A., Goldberg, I., “Distributed key generation for the internet,” Proc. 29th IEEE Int. Conf. on Distributed Computing Systems (ICDCS 90)[9] Montreal, Quebec, Canada, June 2009, pp.119-128.

[9]. Pakniat, N., Noroozi, M., Eslami, Z., “Secret image sharing scheme with hierarchical threshold access structure,” J. Vis. Commun. Image Represent., 2014, 25, (5), pp. 10931101

[10]. Nasrollah Pakniat, Mahnaz Noroozi, Ziba Eslami., “Distributed key generation protocol with hierarchical threshold access structure,” 2014, ISSN 1751-8709

[11]. H. Yan; J. Li; J. Han; Y. Zhang, "A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage," in IEEE Transactions on Information Forensics and Security , vol.PP, no.99,pp.1-1 doi: 10.1109/TIFS.2016.2601070

[12]. G. Murali and R. S. Prasad, "CloudQKDP: Quantum key distribution protocol for cloud computing," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai,2016, pp. 1-6.

[13]. J. Prakash, V. R. Uthariaraj and B. L. Elizabeth, "Efficient KeyManagement Protocol with Predictive Rekeying for Dynamic Networks," 2016 2nd International Conference on Green High PerformanceComputing (ICGHPC), Nagercoil, 2016, pp. 1-6.