A Fine-Grained Access Control Survey For The Secure Big Data Access

Mrs.Naga Kumari Odugu[a], Dr.A.Rajesh[b]

[a] Research Scholar, [b] Associate Professor
[a,b] VELS University,Chennai.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: In this big data era, from different sources a large data can be quickly generated. Access controlling in big data which contains a large amounts data becomes a difficult and challenging task. As per the needs of end users, it is required to build some mechanisms of access control to share the confidential information of end user to a specific authorized user. The main issue in cloud is security for access control. Cloud systems are protected by access control from the security issues. At present Cloud concentrates on various latest researches and implementations, which assures the secured and reliable file transfers. The access controls based on role, attribute, identification and hierarchical based access controls are in existing solutions. These are not enough to trust the cloud computing servers. The further future aim is to secure the files in storage by implementing a trusted model. The main aim of this presented paper is to give a fine-grained access control survey for the secure big data access with others. Access rights are provided by access control, in order to subject exact for object entity set. A set of rights are provided for a certain authorized person is done by Fine grained access control..

Keywords: Fine-grained access control, Big data, Cloud computing, Security

1. Introduction

Cloud is one of the types of computing framework. It provides services which are on-demand with shared computational resource devices and these made lives easier and convenient. For instance, the cloud computing can able to convert a mobile device which is resource constrained into super computer. From the above statement it is clear that the power for a super computation is provided in order to analyze the any information virtually from anywhere in the world from cloud server [1]. As per the above discussion cloud services are benefit to the people. Here, taking software as an example. Presently, the services provided by providers like Google map, Youtube and Facebook and so on are enjoyed by many people. Number of merits is there in Cloud computing i.e., easy scalability, savings in upgrade cost, data access flexibility, disaster recovery and regular backups [2]. Though, there are two drawbacks viz., centralization and security in cloud. Even though it was believed that cloud computing security is improved than the traditional systems security. So in this sense, more resources devoted in solving issues related to security. The critical concern that is from the customers of cloud is unauthorized access for very sensitive data [3].

Generally by encrypting the sensitive content unauthorized access can be avoided generally before the data uploading to the cloud servers. Even though there are many existing challenging issues in practical implementation in systems. Certainly, differentiated access for content is regularly needed in the particular condition when different users having different roles should grant various levels of access. In the past 30 years access control of the data has been developed. Many techniques in access control are developed effectively to implement fine-grained access control; this is able to allow the flexibility in access rights of different individual users [4]. Many numbers of works has been contributing flexibility of access control along with achieving data integrity and scalability. In present scenario vulnerability gaps and potential research remains unaddressed. In this paper first the brief study of cloud storage and the access controlling scheme in it are discussed. Then the three of emerging fine grained access control techniques was reviewed.

2. Cloud Storage and Access Controlling

Cloud computing is an on-demanding service which is provided by particular providers like Amazon, Google, Salesforce.com via internet. Front end cloud computing is done in a new interface service. The storage is not appear to the user and it's maintenance is based on the terms of service providers i.e. the servers maintained by Salesforce.com other than USA but the Google servers maintained in the USA and it is called as back end. The front end and back end of cloud computing can be able to accessed just by connection of internet from any place throughout the world is the advantage this. The data stored in the cloud can be viewed by interface and it is accessible in cloud. Protection is provided thus confidential data which is stored in the cloud cannot be accessed by others [5]. Access control is provided to the data based on the users and data, so access control is accepted to this purpose. Classification of data in cloud is given as public, private and hybrid data. Here private data must comprise of confidential information thus it has data access control. Public data has non-confidential information so no need to higher access control. Lastly for hybrid data may comprise of combinational data as mentioned above therefore it needs security dependency to data [6].

Cloud Storage: A server maintained by the provider company is called Cloud storage. For example, Atmospheric Trace Molecule Spectroscopy (ATMOS) is a storage object for Executive Management Consulting (EMC) Corporation for cloud. Data is stored in the form of objects and those storage objects are able to accessed from anyplace in the world from cloud.

Data sharing: It is not possible to share the data in cloud from one to another place due to the value of cloud storage decreases, because of this reason cloud computing has data sharing and it is an important issue. For efficient data sharing, access control is also used.

Access control: This is used to give control over the subject to object and it is known as access control. Subject may indicate as a person or many. The entity of object can either be software or file or any resource type [7].

Fine-grained Access control: The data is in the servers and software controls the access of data for the people who have access over specific data in existing system and it also checks the authorization for accessing data piece or not. People who have access to server or cloud may leak information so software is not reliable and malicious one. To avoid or to prevent the above problem from the cloud server, fine-grained access control is useful. It is a one of the access control type and in this different people have different rights in accessing for files i.e., according to the identity, a file's access may be provided only to the first person, but not accessed by the other second person. Here Identity may be admin, not only admin, different rights in accessing data provided to every individual. It also ensures that person may access the data piece from the cloud server and it is called as fine-grained access control. It is used in many areas like encrypted attribute searching, records of personal health. There are various access controls, the fine-grained access control is an efficient in decrypting [8].

3. Survey on Fine Grained ACCESS CONTROL SCHEMES

3.1 Multi-Dimensional Fine-Grained Control Authentication Framework

A Multi-dimensional Fine-grained Control (MFC) framework is to strengthen safety and improve RANs (Radio Access Network) is proposed [1]. At first, this was surveyed comprehensively and schemes of existing security to grasp corresponding effects and also disadvantages. Secondly, the framework of MFC is established in order to explain the structural model or implementation processes. Mechanism of mapping identifier is build to attain network isolation. So by using the theoretical comparison of diversified policies, security analysis is performed over MFC. Third, a system of authentication prototype is created in integrated set with parameters settings wireless environment and some particular verification scenarios were illustrated. At last, performance of MFC framework is tested. The results which are valid illustrate the reliability of proposed scheme in controlling the security at end access. Optimization of the performance is done when compared with the multiple schemes, in terms of concurrency and time. Thus, the framework of MFC is feasible in the applications in IoT or 5G.

MFC MODEL: MFC framework has five main modules which are related to the framework that is proposed viz., UTA device, access terminal, IDMS (IDentifier Mapping Server), IAS (Identifier Authentication Server) and IDSR (IDentity Switch Router).

UTA MODULE: It is the medium for user access which is combination of firmware, hardware, upper-layer software, and driver. It also provides function for fingerprint unlocking. In the encrypted device of UTA, AID identifier and digital certificates are stored for authentication identity.

ACCESS TERMINAL: It helps in user in accessing the network comprise registration and login interfaces. There are various terminal categories, along with mobile and fixed devices. Though, standard modules also comprise UTA, configuration management and also user interface module.

IDMS MODULE: This module is useful in storing the entries of mapping to segment in core network along with IP address, , Router Identifier, AID and rights from the side of accessing. The accessing user was located by AID, while to attain separation of core parts and access the dynamically transfers the information of the user by the RID. It was really difficult to leak user information in the network of core.

IDSR MODULE: The module which is present in between the access and core network is IDSR. Along with the forwarding function, It also provides mapping service and also implements system's pre-authentication i.e., conversion of AID to RID. In other hands, the proposed control mechanism of bidirectional is deployed.

IAS MODULE: This is the core part in the framework of MFC, which is used in storing legitimate users information, comprising of User Information (registered UI), AID information respective to UTA, and also rights of user.

The leading entities in the framework are the above given five modules, where terminal is present at the side of user access, while the IDMS and IAS are located at the network side. IDSR module is the handover point in between the network and user space which used in implementation of a distinct mapping in between the RID and AID. In order to ensure the reliability and security after the network accessed by user, in network operation MFC controls the behaviors and rights.

3.2 Fine-grained Big Data Access Control with Privacy-preserving Policy [9]

The big data stored particularly in the cloud structure facing a difficult problem about way of controlling the access of a large quantity of big data. The promising encryption which is enabled by end users is Cipher text-Policy Attribute based Encryption (CP-ABE) to encrypt users own data under access policies which are decided over various attributes of consumers of data and allows just the data consumers whose attributes are going to satisfy the policy access to data decrypt. As in CP-ABE, the plaintext attached to the cipher is the access policy which leaks end users private information. Attribute values are partially hided in access policy, in existing methods yet the names of attributes are not protected. The method that is proposed in the paper is efficient scheme of fine-grained big data access control along with preserving privacy policy. Particularly, in this paper hiding of total attribute in access policies. To help in decryption of data, a new Attribute Bloom Filter was designed to check an attribute whether it is in the policy and to identify exact location in policy. Performance and Security analysis evaluation indicates that this scheme may preserve the privacy policy from Linear Secret Sharing Scheme (LSSS) policy without placing overhead.

The main objective of this paper is to hide total attribute rather than hiding the partial values of attribute. Furthermore, It doesn’t restricts the some particular access structures. Simple idea behind it is to express policy of access in LSSS structure (M,ρ) here M indicates policy matrix, and ρ matches every row Mi of the M Matrix to attribute, and by removing ρ it hides the attributes. It may required to build a localization algorithm of attribute to evaluate the attribute check is in the policy or not, without having the matching attribute function ρ and to locate the accurate location in access policy. Moreover, a new Attribute Bloom Filter is designed to address attributes for the policy of anonymous access, this can save computation cost and storage overhead particularly in big attribute universe.

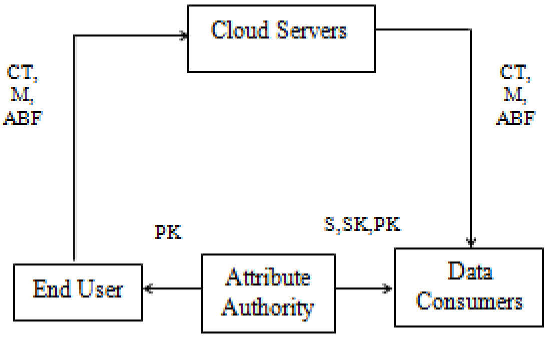

Fig. 1: SYSTEM MODEL

In the present section, firstly, big data sharing and storage models are described. Then, scheme for access control in big data of the proposed system and security model is defined. The access control of the big data system is considered. This system has 5 entities, viz., Cloud Servers, Data Consumers, End-users, and Attribute Authority.

Cloud Servers: These Servers are used to store and to share. It also used to big data processing in system. These are maintained by cloud computing service providers, those are not in the same reliable domain like end-users. So, these servers are not reliable thus the end user’s cannot be trust cloud servers. In order to make and enforce the privacy policy access decisions. Here considering the servers in cloud are not colluding with Data consumers and End-users.

Attribute Authority: This manages every attribute and assigns attributes selected from space attribute to end consumers or end-users. This is the main key generation place, here generation of public parameters are done. The attribute authority grants various access privileges for the end-users by providing secret keys based on the attributes and it is fully trusted in network of a system. **End-user:** These End-users are called as data producers/owners; their data is outsourced in the cloud. Using CP-ABE, these users encrypt their data to control and access their own data. These are considered as honest in the network.

Data Consumers: Data is requested by consumers from cloud computing servers. The data is decrypted by the consumers only when the access policies are satisfied by attributes. Though, the consumer tries to access the inaccessible data from the clouds.

3.3 Fine grained Access Control in Blockchain-Based Framework [10]

The fine grained access control and data privacy challenges faced by the conventional cloud storage system have been addressed by considering the Advanced Encryption Standard (AES) scheme as a significant method. But, a capability is there for PKG called Private Key Generator of an AES scheme in decrypting the total storage data over the cloud that leads to a leakage in privacy data and key abuse problems. Also, a failure in a single point of system can leads to total system collapsing because of the centralized storage working nature of conventional cloud storage model. Then the decentralized storage model is came into exists by developing the technology called blockchain. There are various advantages with this decentralized model like higher throughput, lower cost along with overcame by the failure of single point problem in system compared to the conventional cloud storage system. Therefore, this paper [10] studied about the decentralized storage system with the data storing and sharing schemes. A framework also developed in this which integrates the Ethereum blockchain and decentralized storage Interplanetary File System (IPFS) with the ABE technology as shown in figure (2).

The Data owner (DO) and Data user (DU) are the two types of entities include in this system. The DO can be either an organization or a person which was the owner for a series of files to share. Whereas DUs are the authorized data clients of DOs who were allowed to access some of those files. But the nodes of IPFS storage and Ethereum blockchain's minors were not come under this. The framework of this system shown in figure (2) clearly illustrating that a block chain is developed with a smart contract for fine grained access control indicting by a double arrow pointed to the smart contract

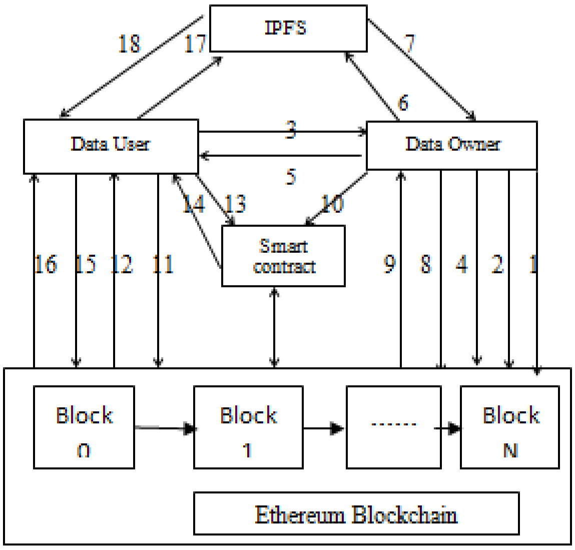

Fig. 2: BLOCKCHAIN-BASED FRAMEWORK WITH FINE GRAINED ACCESS CONTROL

The description corresponding to the each numbered step from the figure (3) can be given as,

1 represents the system setup by the DO and embedding of an encrypted master key of system into the Ethereum transaction.

2 represent the deployment of smart contract through DO for Ethereum blockchain.

3 represent the registration request sent by the DU to the DO.

4 represent the embedding of a secrete key that generated by Do and encrypted with the shared key for the Du into the Ethereum transaction.

5 smart contract ABI, source code, and secret code related to transaction sent by DO to DU via secured channel.

6 A keyword from the file which is shared is selected and uses algorithm of AES to encrypt by DO and uploaded to IPFS.

7 File location which is returned by IPFS was recorded by DO.

8 DO use a chosen AES K key and ABE algorithm to encrypt the location of file and AES K. After this AES key K1 is selected to encrypt information and also to embed it to transaction Ethereum.

9 AES K1 key and Ethereum transaction id recorded by DO.

11 The transaction data which is associated with the secret key is read by DU from Ethereum blockchain.

12 Shared key is used to decrypt the data transaction by DU after that it gets the secret key.

13 Search token was generated and smart contract is invoked by the DU.

14 Based on the token, smart contract searches and returns the related results.

15 Smart contracts returns the data transaction based on the results of search.

16 Transaction data was decrypted by DU.

17 The encrypted files were downloaded by DU from IPFS.

18 The encrypted file was decrypted by DU.

The fine grained access control is achieved over the data in the above framework and a secret key distribution capability to the data users is there by the data owner with encrypting the data that was shared through specifying the access policy. The conventional cloud storage systems facing a problem of return the incorrect search results or not return the total search results can solved by the implemented decentralized system model with the cipher text based key-word search function in accordance with the smart contracted Ethereum blockchain. Then lastly, this method is simulated under the Ethereum official test network on the linux operating system.

4. Results

The table (1) depicts the comparative analysis of fine grained access control schemes that are reviewed in this paper. so this was compared with scheme that ehich was proposed with other access control schemes.

Table 1: Comparative Analysis Of Surveyed Fine Grained Access Control Schemes

Scheme Parameters	[1]	[9]	[10]
Fine-grained Access Control	Multi Access	yes	yes
Decentralized storage	yes	yes	yes
Type of Access Control	ABE	CP-ABE	AES
Privacy Authentication	UTA network access device	Privacy policy	Ethereum blockchain

In addition, above analysis, compared the cost of time in survey control schemes in terms of number of registered users. In figure (3), a comparison in delay is presented, as the number of users increased. From the figure (3), it is clear that the Multi-Dimensional Fine-Grained Control scheme has the lowest authentication delay, and Fine-grained Big Data Access Control scheme delay is similar to the Blockchain-Based based Fine grained Access Control scheme. Even before the number of users reached 700, the Blockchain-Based based Fine grained Access Control solution was superior to the framework Multi-Dimensional Fine-Grained Control proposed. Since the increase rate of the Multi-Dimensional Fine-Grained Control scheme is less than that of Fine-grained Big Data Access Control and Blockchain- based Fine grained Access Control is the proposed scheme which is optimal if and only if the number is greater than 700.

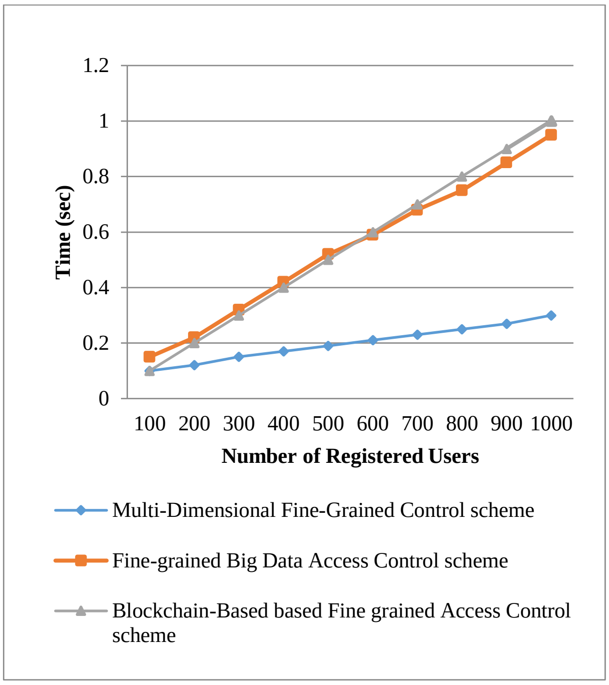

Fig. 3: Time Cost Of Different Access Control Schemes

5. Conclusion

At present, traditional cloud storage may cause the data of the user to be not available because of force factors in majeure (like natural disasters, government censors, etc.). To protect the availability and privacy of data, to decentralized cloud storage systems it is necessary to transfer the data sharing and storage from the cloud storage which is centralized and decentralized storage has literally low prices compared to traditional storage with the merit of the huge data throughput. It is required to stop worrying on single point failure. The ABE technology and searchable encryption technology on cipher text are important technologies for solving privacy of data and fine grained access control problems. The survey on fine-grained access control schemes is presented in this paper. Through this, the overall view of fine-grained access control system can obtained..

References

Ying Liu, Zhengyang Ai, , Fuhong Li Fei Song and Liu Chang, “A Smart Collaborative Authentication Framework for Multi-Dimensional Fine-Grained Control”, IEEE Access, January 15, 2020.

Naixue Xiong Jingli Ren and Pan Yang, “Data Security and Privacy Protection for Cloud Storage: A Survey”, IEEE Access Volume: 8, 2020

Jin Sun, Yi Zhang, Zebin Wu, Yaoqin Zhu, Zhongzheng Ding, Xianliang Yin, Javier Plaza, Zhihui Wei, and Antonio Plaza,” An Efficient and Scalable Framework for Processing Remotely Sensed Big Data in Cloud Computing Environments”, IEEE Trans. Geo science and Remote Sensing, Vol: 57, Issue: 7, 2019.

Sandip Roy, Samiran Chattopadhyay, Neeraj Kumar, Ashok Kumar Das, Joel J. P. C. Rodrigues, Santanu Chatterjee, “Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications”, IEEE Trans. on Industrial Informatics, Vol: 15, Year: 2019.

Lei Xu, , Seung Hun Kim,Qingji Zheng, Taeweon Suh, Shouhuai Xu, JongHyuk LeeWon Woo Ro, Weidong Shi, “Architectural Protection of Application Privacy against Software and Physical Attacks in Untrusted Cloud Environment”, IEEE Transactions on Cloud Computing, 2018.

Hao Jin, Ke Zhou, and Hong Jiang“Dynamic and Public Auditing with Fair Arbitration for Cloud Data”, IEEE Trans. on Cloud Comp. vol:6, Issue:3, 2018.

Yingjie Xue, Kaiping Xue, Wei Li, Hao Yue, Jianan Hong, Peilin Hong, David S.L. Wei, “RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage”, IEEE Trans. on Information Forensics and Security, Vol”:12, Issue:4, 2017.

Qi Han, Kan Yang, Kan Zheng, Hui Li, Xuemin Shen, Zhou Su, “An Efficient and Fine-Grained Big Data Access Control Scheme With Privacy-Preserving Policy”, IEEE Internet of Things Journal, Volume:4, Issue:2, 2017

Qi Han, Kan Yang, Kan Zheng, Hui Li, Xuemin Shen and Zhou Su, “An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy”, IEEE Internet of Things Journal, 2016.

Yinglong Zhang, Shangping Wang, Yaling Zhang, “A Blockchain-Based Framework for Data Sharing with Fine-grained Access Control in Decentralized Storage Systems”, , IEEE Access, Vol 4, 2016

Y. M. Tseng, S. S. Huang, J. H. Ke, and T. T. Tsai, "List-free ID-based mutual authentication and key agreement protocol for multiserver architectures", IEEE Transactions on Emerging Topics Computing, volume 4, no. 1, pp. 102-112, Jan.–Mar. 2016.

L. A. Tawalbeh, W. Bakhader, R. Mehmood and H. Song, "Cloudlet-Based mobile cloud computing for healthcare applications", Proc. IEEE Global Commun. Conf., pp. 1-6, 2016.

S. Chatterjee, A. K. Gupta and G. Sudhakar, "An efficient dynamic fine grained access control scheme for secure data access in cloud networks", Proceedings. IEEE Int. Conf. Electronics and Computer Communication. Technol. (ICECCT), pp. 1-8, Mar. 2015.

X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security", IEEE Transactions on Computing., volume. 64, no. 4, pp. 971-983, Apr. 2015.

J. Baek, Q. H. Vu, J. K. Liu, X. Huang and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid", IEEE Transactions on Cloud Computing, volume. 3, no. 2, pp. 233-244, Apr./Jun. 2015.