AN ATTRIBUTE-BASED CONTROLLED COLLABORATIVE ACCESS CONTROL SCHEME FOR PUBLIC CLOUD STORAGE

N.SRINIVASA RAO [1] **SUNKARA RAMA NARASIMHA RAO**[2].

[1] Assistant Professor, **DEPT OF MCA, SKBR PG COLLEGE , AMALAPURAM, Andhra Pradesh**

Email:- naagaasrinu@gmail.com

[2]**PG Student of MCA, SKBR PG COLLEGE , AMALAPURAM, Andhra Pradesh**

Email:- ramanarasimha.1sunkara@gmail.com.

ABSTRACT

In public cloud storage services, data are outsourced to semi-trusted cloud servers which are outside of data owners' trusted domain. To prevent untrustworthy service providers from accessing data owners' sensitive data, outsourced data are often encrypted. In this scenario, how to conduct access control over these data becomes a challenging issue. Attribute based encryption (abe) has been proven to be a powerful cryptographic tool to express access policies over attributes, which can provide a fine-grained, flexible, and secure access control over outsourced data. However, existing ABE-based access control schemes do not support users to gain the access permission by collaboration. In this paper, we explore a special attribute-based access control scenario where multiple users having different attribute sets can collaborate to gain access permission if the data owner allows their collaboration in the access policy. Meanwhile, the collaboration that is not designated in the access policy should be regarded as a collusion and the access request will be denied. We propose an attribute-based controlled collaborative access control scheme through designating translation nodes in the access structure. Security analysis shows that our proposed scheme can guarantee data confidentiality and has many other critical security properties. Extensive performance analysis shows that our proposed scheme is efficient in terms of storage and computation overhead.

INTRODUCTION

Cloud computing has emerged as the natural evolution and integration of

advances in several fields, including utility computing, distributed computing, grid computing, and service oriented architecture . It promotes the concept of leasing remote resources rather than buying hardwares, which frees cloud customers (such as enterprises and individuals) from maintenance expenses. Cloud customers are able to utilize cloud services on a pay-as-you-use basis, where the price is relatively low. What's more, since services are provided via the Internet, customers can access applications and data anywhere and anytime. To benefit from the above advantages, but not limited to, an increasing number of enterprises and individuals are willing to outsource their data and applications to cloud platforms. Despite many advantages of cloud computing, there still remain various challenging issues that impede cloud computing from being widely adopted, among which, privacy and security of users' data have been the major issues. Traditionally, a data owner stores his/her data in trusted servers which are generally controlled by a fully trusted administrator. However, in public cloud storage, which is a popular service model in cloud computing, data are usually stored and managed on remote cloud servers which are administrated by a semi-trusted third party, i.e. the cloud service provider. Data are no longer in data owners' trusted domains and they cannot trust cloud servers to conduct secure data access control. Therefore, the secure access control has become a challenging issue in public cloud storage, in which traditional security technologies cannot be directly applied. In recent years, many researchers have been devoted on data access control in public cloud storage, such as the work in . Among those literatures, Ciphertext-policyAttribute-based Encryption (CP-ABE) is regarded as one of the most suitable schemes due to the fact that it can guarantee data owners' direct control over their data and provide a fine-grained access control service. In CP-ABE schemes, each user is associated with a set of attributes and every ciphertext is embedded with an access structure over some chosen attributes. [3] discussed about a method, This scheme investigates a traffic-light-based intelligent routing strategy for the satellite network, which can adjust the pre-calculated route according to the real-time congestion status

of the satellite constellation. In a satellite, a traffic light is deployed at each direction to indicate the congestion situation, and is set to a relevant color, by considering both the queue occupancy rate at a direction and the total queue occupancy rate of the next hop. The existing scheme uses TLR based routing mechanism based on two concepts are DVTR Dynamic Virtual Topology Routing (DVTR) and Virtual Node (VN). In DVTR, the system period is divided into a series of time intervals. On-off operations of ISLs are supposed to be performed only at the beginning of each interval and the whole topology keeps unchanged during each interval. But it has delay due to waiting stage at buffer. So, this method introduces an effective multi-hop scheduling routing scheme that considers the mobility of nodes which are clustered in one group is confined within a specified area, and multiple groups move uniformly across the network

RELATED WORK

1) DAC-MACS: Effective data access control for multi-authority cloud storage systems

AUTHORS: K. Yang, X. Jia, K. Ren, and B. Zhang

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to data access control for multi-authority cloud storage systems, due to the inefficiency of decryption and revocation. In this paper, we propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new

multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security. The analysis and the simulation results show that our DAC-MACS is highly efficient and provably secure under the security model.

2) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption

AUTHORS: M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme. [2] discussed about a

method, End-to-end inference to diagnose and repair the data-forwarding failures, our optimization goal to minimize the faults at minimum expected cost of correcting all faulty nodes that cannot properly deliver data. First checking the nodes that has the least checking cost does not minimize the expected costin fault localization. We construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. We proposes efficient inferring approach to the node to be checked in large-scale networks.

SYSTEM ANALYSIS

EXISTING SYSTEM:

J. M. M. Perez et. al. pointed out that ABE schemes cannot express access control rules like role hierarchy and object hierarchy. Consequently, they proposed a secure role-based access control scheme to address the problem.

S.-C. Yeh, developed a system and their main goal is to assign different privileges (such as read, write, and grant) to different users. A user can obtain privilege independently. The works that have the concept of collaboration that are most similar to ours are found in the research area of online social networks.

DISADVANTAGES OF EXISTING SYSTEM:

They are either coarse-grained or short of scalability as the number of users increases.

The existing CP-ABE schemes can merely assign access permission to individuals who own attribute sets satisfying the access policy. However, in many scenarios, the secret information cannot be obtained individually by a single user alone.

PROPOSED SYSTEM:

In this paper, we address the collaboration issue in practical scenarios and propose an attribute-based controlled collaborative access control scheme for public cloud storage.

In our work, in order to provide both data confidentiality and collaborative access control, only people who are in charge of the same project are allowed to collaborate. Technically, data owners allow expected collaboration by designating translation nodes in the access structure. In this way, unwanted collusion can be resisted if the attribute sets by which users are

collaborating are not corresponded to translation nodes.

For colluding users across groups, their access is not permitted as their secret keys do not correspond to the same group.

ADVANTAGES OF PROPOSED SYSTEM:

We address the problem of data access control in collaboration scenarios and propose an attribute-based controlled collaborative access control scheme. Data owners can specify expected collaboration among users when they define access policies. Meanwhile, unwanted collusion can be denied to access the data.

We design a mechanism to achieve our goal by designating translation nodes in policy trees and modifying secret keys and ciphertexts. More specifically, our approach embeds a translation key inside the secret key of BSW scheme and adds a translation value in the ciphertext for each translation node. The combination of translation keys and translation values enables users to collaborate to satisfy a policy tree.

Users are divided into groups in a way such that the collaboration is restricted and secure. That is to say, only users responsible for the same project are allowed to collaborate in case that malicious users who are not responsible for the project collude. Extensive security analysis is given to show the security properties of our proposed scheme.

MODULES:

- The central authority (CA)
- The data owner (Owner)
- The data consumer (User)
- Cloud servers

MODULES DESCSRIPTION:

The central authority (CA)

The central authority (CA) is the administrator of thewhole system. Particularly, it sets up the system parametersfor the access control implementation and distributessecret keys for users.

The data owner (Owner)

The data owner (Owner) is the entity who outsourceshis/her data to cloud servers. To share his/her data withother intended entities, he/she defines access policiesfor data. The access policy is represented by an

accessstructure over attributes. Data contents are encryptedunder access structures before being uploaded to cloudservers.

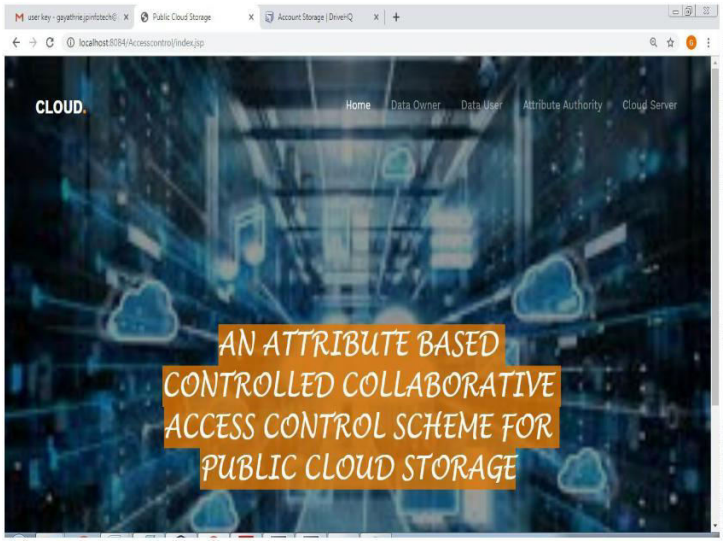
The data consumer (User)

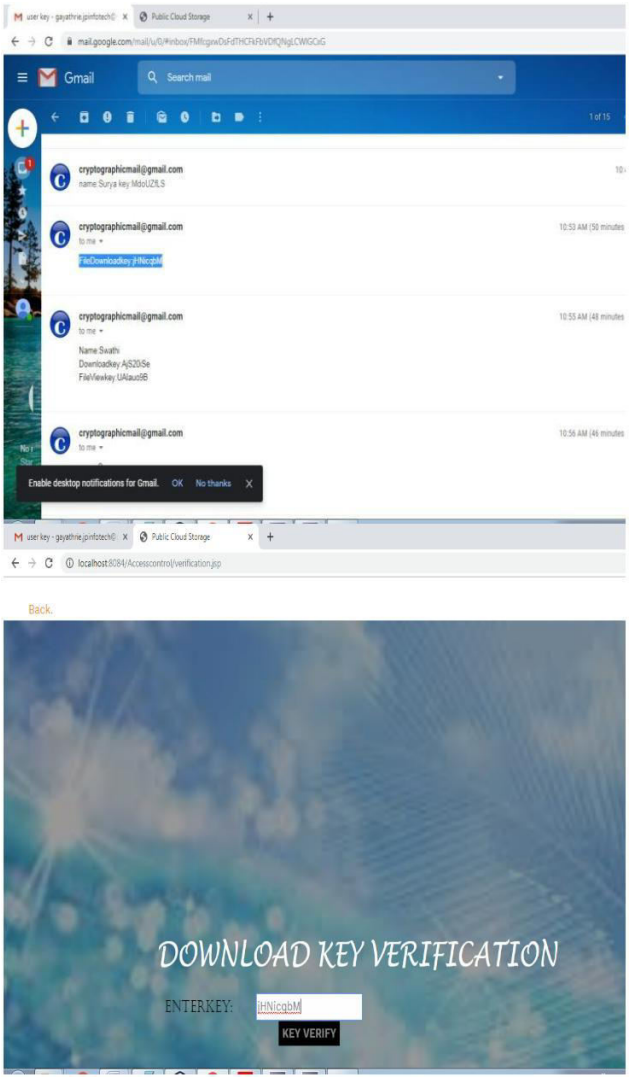
The data consumer (User) is the entity who is interestedin data contents. In our controlled collaborative accesscontrol scheme, each user is assigned to a group relatedto the project for which he/she is responsible. He/She possesses a set of attributes and is equipped with a secretkey associated with his/her attribute set. The user can freely get any encrypted data that he/she is interested in from cloud servers. Then, he/she can decrypt the encrypted data on either conditions: (1) His/Her attribute set independently satisfies the access structure embedded inside the encrypted data; (2) If the policy allows/specifies some kinds of collaboration, he/she can collaborate withother valid users to decrypt the data.

Cloud servers

Cloud servers provide a public platform for owners to store and share their encrypted data. They do not conduct data access control for owners. The encrypted data stored in cloud servers can be downloaded freely by any data consumer.

SCREENSHOT





CONCLUSION

In this paper, we proposed an attribute-based controlled collaborative access control scheme, in which data owner scan designate selected users to collaborate for accessing their data at their will. Considering practical scenarios, we let users within the same group to collaborate for data access. More importantly, the data owner can devise the way for chosen users to combine their attribute sets to satisfy the access policy ,and at the same time also resist the collusion attack when curious users try to combine their attribute sets in other ways. Technically, we embed translation keys in the secret keys of CP-ABE schemes and modify the secret keys to associate groups to users. The data owner can designate collaboration by setting translation nodes in the policy tree. Our security analysis shows that our proposed scheme effectively supports data confidentiality, user collusion resistance, controlled collaboration within the same group, secret key privacy, securer vocation of the collaboration and non-reusability of intermediate results. The performance is very satisfactory. Thus, our proposed scheme is highly promising to provide fine-grained access control in collaborative settings where data need to be accessed by multiple users.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz,A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoicaet al., "A view of cloud computing," Communications ofthe ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] Christo Ananth, Mary Varsha Peter, Priya.M., Rajalakshmi.R., Muthu Bharathi.R., Pramila.E., "Network Fault Correction in Overlay Network through Optimality", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Volume 2, Issue 8, August 2015, pp: 19-22.

[3] Christo Ananth , P.Ebenezer Benjamin, S.Abishek, "Traffic Light Based Intelligent Routing Strategy for Satellite Network", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.24-27.

[4] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access toscalable media in cloud-assisted content sharing," IEEETransactions on Multimedia, vol. 15, no. 4, pp. 778–788,2013.

[5] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, andP. Hong, "RAAC: Robust and auditable access controlwith multiple attribute authorities for public cloud storage,"IEEE Transactions on Information Forensics andSecurity, vol. 12, no. 4, pp. 953–967, 2017.