International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Privacy Preserving Searchable Encryption with Role Based Access Control

Dr.T.Ganesan[1] ,A.Akila[2], A.Jaya[3], M.Thamizhpriya[4]

[1]Professor,EGS Pillay Engineering College, Nagapattinam, Tamil Nadu, India.
[2]Ug, Student, EGS Pillay Engineering College, Nagapattinam, Tamil Nadu, India.
[3]Ug, Student, EGS Pillay Engineering College, Nagapattinam, Tamil Nadu, India.
[4]Ug, Student, EGS Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

ABSTRACT

Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. In cloud computing, cloud service providers compromise an abstraction of infinite storage space for clients to mass data. It can help clients diminish their financial overhead of data managements by drifting the local managements system into cloud servers. However, security concerns develop the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a mutual approach is to encrypt data files before the clients upload the encrypted data into the cloud. Cloud storage services can help clients reduce their monetary and maintenance overhead of data managements. It is complex to design a secure data sharing scheme, especially for dynamic groups in the cloud. To overcome the problem, here propose a secure data sharing scheme for frequently changed groups. In this work, an AES based encryption scheme is proposed which incorporates the cryptographic approaches with Group Data Sharing and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. If the group member can be revoked means, automatically change public keys of existing group and no need encrypt again the original data. Any user in the group can access data source in the cloud and revoked users does not allowed accessing the cloud again after they are revoked. Finally implement this secure distribution scheme into group data sharing environments.

Keywords:Cloud computing, Access control, Searchable encryption, Cloud security, Data sharing

I. INTRODUCTION

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data. Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of layered defense to protect access control systems. These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or IP address. Directory services and protocols, including the Local Directory Access Protocol (LDAP) and the Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers. Organizations use different access control models depending on their compliance requirements and the security levels of information technology they are trying to protect.

1.1. Structure

1. Advantages of Cloud Based Access Control Systems

Interest in cloud-based access control has surged in recent years, attracting businesses of different sizes and across industries. For anyone who has been seen the benefits of cloud-based systems, that's hardly a shock. From streamlined system management to pricing flexibility, cloud-based access control offers some very attractive qualities when compared with traditional, on- premise systems. Some key examples are listed below.

2. *Accessibility from anywhere with an Internet connection*

While some traditional access control systems offer some remote connectivity, cloud systems are designed with mobile accessibility in mind. Authorized users can log into the relevant access control app, web portal, or network to view or manage system activity. Aside from providing convenience, this also enables users to receive alerts and take action in the field in the event of an incident or emergency.

3. *Flexible cost management*

Whereas traditional access control systems often come with high upfront installation and equipment costs, cloud-based services provide much greater flexibility in pricing. Instead of purchasing on-site equipment outright, users can opt to lease equipment from an authorized reseller, avoiding high capital expenditure costs in favor of modest ongoing operational costs.

4. *Reduced burden on user staff*

Maintaining a business system takes time and effort, particularly for mission-critical ones like access control. By turning over the hosting and maintenance of on-site PCs, servers, data-redundancy infrastructure and related processes to the integrator, users can dramatically decrease the burden on their own IT staff. Depending on the application itself, a cloud-based system can reduce IT involvement by 97%. Should the user desire, management of the cloud system can be turned over partially or fully to the integrator as well.

5. *System reliability*

Storing all data on site can be quite risky: unless the user has strong safeguards in place, a power surge or network failure can impact system operation or result in the destruction of that data. To that end, cloud-based access control systems generally utilize centralized data centers that are equipped with robust backup power and storage systems to ensure the safety and integrity of the system and data.

6. *Round-the-clock updates and monitoring*

Software updates and patches are critical for ensuring that the access control system is up to date and that any vulnerability is addressed. However, these updates are only helpful if they are implemented in a timely manner. With cloud-based access control systems, updates can be pushed out quickly and simultaneously across system devices, rather than requiring employees to handle them. This helps increase system efficiency and security, while decreasing the risk of human error. In addition, many cloud-based systems offer 24/7 monitoring services, helping improve response time, provide peace of mind and free up end user staff to tackle more pressing business challenges. As with traditional access control, cloud-based solutions vary from business to business, as do the benefits that users care most about. Perhaps the most exciting benefit of all is that users can find new ways to not only strengthen facility security, but also optimize IT and other operations business-wide.

II. RELATED WORKS

Fu, Anmin, et.al,…[1] proposed a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least t group managers to recover a trace key cooperatively, which eliminates the abuse of single-authority power and provides nonframeability. Here establish a model for data (in a group) shared with multiple group managers, and propose a new privacy preservation public auditing scheme for multiple group managers in shared cloud storage. This proposed scheme can not only provide multi-levels privacy-preservation abilities (including identity privacy, traceability and non-frame ability), but also can well support group user revocation. And design a data structure based on a binary tree for clouds to record all the changes of data blocks. Group users can trace the data changes through the binary tree and recover the latest correct data block when the current data block is damaged. And utilize an authorized authenticate process to verify TPA's challenge messages. Therefore, only the TPA who has been authorized by the group users can pass the authentication and then challenge the cloud, which protects clouds from malicious challenges.

Jiang, Tao, et.al,…[2] provided an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the scheme definition. Group users consist of a data owner and a number of users who are authorized to access and modify the data by the data owner. The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users. The TPA could efficiently verify the integrity of the data stored in the cloud storage server, even the data is frequently updated by the group users. The data owner is different from the other group users, he/she could securely revoke a group user when a group user is found malicious or the contract of the user is expired. In this case, although the server proxy group user revocation way brings much communication and computation cost saving, it will make the scheme insecure against a malicious cloud storage server who can get the secret key of revoked users during the user revocation phase. Thus, a malicious cloud server will be able to make data m, last modified by a user that needed to be revoked, into a malicious data. In the user revocation process, the cloud could make the malicious data m′ become valid.

Pritam, Divya, et.al,…[3] implemented an encryption scheme which incorporates the cryptographic approaches with RBAC and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. A real-time method is provided to maintain a secure communication in cloud computing which ensures security as well as trust-based access to cloud. The proposed model contains algorithms to explain data protection and user authentication problems. A secure RBAC based cloud storage system is proposed in this paper. In our system, the Data Owner encrypts the data in such a way that only the Data Users with relevant access policies can decrypt and view the data. The cloud service provider (who stores the data) will not be able to see the content of the data without the specified access policy. To prevent the admission of malicious Data Owner to cloud, an Admission Policy is proposed. Based on this policy, only genuine Data Owners can get admission to cloud which is based on voting by existing Data Owners. The authentication mechanism plays a vital role in security enhancement. Authentication mechanism is like an entrance door and will allow only the trusted individuals to enter in the cloud premises. The mechanism should be robust enough to ensure availability by letting the right person in, any time and any place. Authentication mechanism can be combined with cryptographic techniques to ensure confidentiality of data.

Krishna, Ch M. Siva Rama, and G. John Samuel, et.al,…[4] considered the problem using Attribute-Based Encryption (ABE) in a setting where users' credentials may change and ciphertexts may be stored by a third party. Our main result is obtained by pairing two contributions: – We first ask how a third party who is not trusted with secret key information can process a cipher text to disqualify revoked users from decrypting data encrypted in the past. Our core tool is a new procedure called cipher text delegation that allows a cipher text to be're-encrypted' to a more restrictive policy using only public information. KP-ABE is a public key cryptography primitive for one to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encrypt or associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfil his access structure.The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and downloading of a file to a cloud with standard Encryption/Decryption is more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future. The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes

Sahai, Amit, et.al,…[5] motivated by the question of access control in cloud storage, we consider the problem using Attribute-Based Encryption (ABE) in a setting where users' credentials may change and ciphertexts may be stored by a third party. Our main result is obtained by pairing two contributions: – We firstask how a third party who is not trustedwith secret key information can process a cipher text to disqualify revoked users from decrypting data encrypted in the past. Our core tool is a new procedure called cipher text delegation that allows a cipher text to be‘re-encrypted’ to a more restrictive policy using only public information. Second, we study the problem of revocable attribute-based encryption. Here provide the first fully secure construction by modifying an attribute-based encryption scheme and prove security in the standard model. We then combine these two results for a new approach for revocation on stored data. Our scheme allows a storage server to update stored ciphertexts to disqualify revoked users from accessing data that was encrypted before the user’s access was revoked while key update broadcasts can dynamically revoke selected users.Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead.

III. Existing methodologies

Existing system proposed an attribute-based controlled collaborative access control scheme for public cloud storage. Restrict user collaboration in the same group that corresponds to the same project for which the involved people are responsible. Thus, in proposed work, in order to provide both data confidentiality and collaborative access control using IBE (Identity Based Encryption), 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. Using this translation value and special translation keys embedded in users’ secret keys, users within the same group can collaborate to satisfy the access structure and gain the data access permission. For colluding users across groups, their access is not permitted as their secret keys do not correspond to the same group. 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 those malicious users who are not responsible for the project collude. Extensive security analysis is given to show the security properties of our proposed scheme. In existing scheme, the security assumptions of the four roles can be defined as follows. Cloud servers are always online and are managed by the cloud provider who is usually assumed to be “honest-but-curious”. It means that cloud servers will correctly execute the tasks assigned to them for profits, but they would try to obtain as much secret information as possible based on data owners’ inputs and outsourced data. CA is assumed to be fully trusted, which will not collude with any entity to peep data contents.

IV. PROPOSED METHODOLOGIES

A new method known as Role Based Access Control (RBAC) was introduced. Role based Access Control (RBAC) determines user’s access to the system based on the Job role. The role a user is assigned to be basically based on the least privilege concept. The role is defined with the least amount of permissions or functionalities that is necessary for the job to be done. Permissions can be added or deleted if the privileges for a role change. However, problems became apparent when RBAC was extended across administrative domains. The data owner can specify a group of users that are approved to view his or her data. Any time the member of the group must access the data without the data owner’s interference. Only data owner and the members of the group should access the data, no other can access the data including the Cloud Service Provider. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. The data owner gets back the permission to access data for any member of the group. The data owner can add new user to the group. The member of the group must not be allowed to revoke rights of other members of the group or add new users to the group. The data owner has to specify who has read/write permissions on the data owner’s files.

Cloud Framework Construction

There are three key parties in an RBAC model. First, Data Owner (DO) who intend to share and store their information or resources in the cloud; second, users who need to access the owners’ shared resources; and third, roles that grant access levels to cloud users who are registered to use the shared resources. In this RBAC system model, first, owners, who are service providers (SPs), share their resources/services with roles based on roles’ trust level. Next, the registered users in roles can access the shared resources/services.

Data Upload and Encryption

DO is a cloud client who registers with the CSP (Cloud Service Provider).DO outsources data to cloud in encrypted form. DO anonymously get authenticated to cloud while getting duly authenticated. It is the duty of the DO to prevent the admission of malicious DO's to cloud. The encrypted data is uploaded to the cloud by the Data Owner. The DO can encrypt the file using AES encryption technique. The choice of encryption is of the DO.

AES Encryption

The AES cipher is also known as the block cipher. No successful attack has been reported on AES. Some advantages of AES are easy to implement on 8-bit architecture processors and effective implementation on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). AES encryption is performed in multiple rounds. Each round has four main steps including sub-byte, shift row, mix column and add round key. Sub-byte is the substitution of bytes from a look-up table. Shift row is the shifting of rows per byte length. Mix column is multiplication over Galois field matrix. Finally, in the add round key step, the output matrix of mix column is XORed with the round key. The number of rounds used for encryption depends on the key size. For a 128-bit key, these four steps are applied to 9 rounds, where the 10th round does not consider the mix column step. Since all steps are recursive, decryption is the reverse of encryption.

Algorithm Procedure

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

Role based access control

RBAC is nothing more than the idea of assigning system access to users based on their role within an organization. The system needs of a given workforce are analysed, with users grouped into roles based on common job responsibilities and system access needs. Access is then assigned to each person based strictly on their role assignment. With tight adherence to access requirements established for each role, access management becomes much easier.

Data Access

The user or specific member wants to download a file they should have shared secret key distributed from data owner (Manager). Then gives the file name and enter the secret key. During the process of key verification user's role also verified by the server system. If secret key and user's role are valid then they are allowed to decrypt this downloaded file.

User Revocation

Once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user and intimate PKG to generate re-signing key. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block.

V. EXPERIMENTAL RESULTS

The proposed system can be implemented in ASP.NET framework as Front and SQL server as Back End. The performance of the project can be defined as follows:

Proof Generation Time:

From the execution of proposed algorithm, the time complexity for generating proof for data blocks (50; 100; 200; 400; 500) from the mean of 20 trails is calculated. The variation in the computation for large number of files could not be determined because of the limits on the configuration of the device. The average proof generation time will be shown in below figure

	Proof Generation Time (sec)	
	Existing	**Proposed**
Number of Blocks		
100	1.2	0.8
200	2.3	1.4
300	3.4	1.8
400	4.5	2.5
500	5.5	3.0

Table 1: Performance table

Proof Verification Time:

From the execution of proposed algorithm, the time complexity for proof verification of data blocks (50; 100; 200; 400; 500) from the mean of 20 trails is calculated. The variation in the computation for large number of files could not be determined because of the limits on the configuration of the device. The average proof verification time will be shown in below graph.

	Existing	**Proposed**
Number of Blocks		
100	0.25	0.42
200	0.5	0.75
300	0.8	1.2
400	1.025	1.5
500	1.65	1.9

Table 2: Proof verification time

From the above table, proposed system provide the reduced time to encrypt and decrypt the data than the existing system

VI. CONCLUSION

Data sharing in the Cloud is available in the future as demands for data sharing continue to grow rapidly. Proposed work, presented a review on secure data sharing in cloud computing environment. To reduce the cost data owner outsource the data. Data owner is unable to control over their data, because cloud service provider is a third party provider. The problem with data sharing in the cloud is the privacy and security issues. Various techniques are discussed in this paper to support privacy and secure data sharing such as AES encryption, Group data sharing and User revocation. The study concludes that secure anti-collision data sharing scheme for groups provides more efficiency, supports access control mechanism and data confidentiality to implement privacy and security in group sharing. Proposed work also supports to provide efficient integrity auditing of shared data, user revocation and supports batch auditing. TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

References

[1] Fu, Anmin, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang. "NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users." IEEE Transactions on Big Data (2017).

[2] Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma. "Public integrity auditing for shared dynamic cloud data with group user revocation." IEEE Transactions on Computers 65, no. 8 (2015): 2363-2373.

[3] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Enforcing role-based access control for secure data storage in the cloud." The Computer Journal 54, no. 10 (2011): 1675-1687.

[4] Ruj, Sushmita,. "Decentralized access control with anonymous authentication of data stored in clouds." IEEE transactions on parallel and distributed systems 25, no. 2 (2013): 384-394.

[5] Sahai, Amit, Hakan Seyalioglu, and Brent Waters. "Dynamic credentials and ciphertext delegation for attribute-based encryption." In Annual Cryptology Conference, pp. 199-217. Springer, Berlin, Heidelberg, 2012.

[6] Guo, Rui, Huixian Shi, Qinglan Zhao, and Dong Zheng. "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems." IEEE Access 6 (2018): 11676-11686.

[7] Dagher, Gaby G.. "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology." Sustainable Cities and Society 39 (2018): 283-297.

[8] Mehmood, Abid, Iynkaran Natgunanathan, Yong Xiang, Howard Poston, and Yushu Zhang. "Anonymous authentication scheme for smart cloud based healthcare applications." IEEE access 6 (2018): 33552-33567.

[9] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42, no. 8 (2018): 152.

[10] Sun, You, Rui Zhang, Xin Wang, Kaiqiang Gao, and Ling Liu. "A decentralizing attribute-based signature for healthcare blockchain." In 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1-9. IEEE, 2018.