Enforcing Role-Based Access Control for Secure Data Storage in Cloud Using Authentication and Encryption Techniques

Divya Pritam
M.E. Student, Department of Computer Engineering,
Pillai Institute of Information Technology, New Panvel, Mumbai, India.

Madhumita Chatterjee
Professor, Department of Computer Engineering
Pillai Institute of Information Technology, New Panvel, Mumbai, India.

Abstract – With the fast advancement taking place in cloud computing and services, the culture to use the cloud for large-scale data storage is being adopted. This growth in cloud computing has elevated the key security issue of how to control and avert illegitimate access to data stored in the cloud. Now a days most of the work concentrates on privacy of data contents and access control, whereas the attention towards privilege control is compensated. Role-based access control (RBAC) is one of the familiar access control model which provides flexible controls and database management by having users mapped to roles and roles mapped to privileges on data objects. In this paper, an encryption scheme is proposed 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. The analysis suggests that the purpose of this work is carried out by the proposed algorithm i.e. to decrease cloud computing security concerns such as data protection, authentication, and securing data while communicating.

Index Terms – Cloud computing, Security, Encryption, User Authentication, Role-based access control, Admission Policy.

1. INTRODUCTION

Cloud storage is an evolving paradigm, shifting the storage capabilities and computing to cloud service providers. Due to the loss of direct control on the outsourced data, companies and customers raise more and more concerns about the security and privacy [1] [2] of cloud systems. Protecting data and business in the cloud is vital to all the cloud clients. As the sensitive data of users is presented to remote server machines which are purchased and operated by third party service providers in unencrypted forms, the risks of unauthorized leakage of the user's sensitive data by service providers may be quite high. Therefore, several security mechanisms have to be set up in order to cope with the emerged cloud concerns namely outsourcing encrypted data and periodically checking the data integrity and availability.

Effective security measures have to be taken while considering outsourcing data to cloud services. Preventing unauthorized access of sensitive data in cloud has been one of the biggest challenges while designing a secure cloud system. One of the techniques to protect user's data from outside attackers is to protect the confidentiality of data from service providers which ensures that the cloud service provider cannot collect the confidential data of the user during its processing as the data is stored in cloud computing systems. When dealing with cloud, confidentiality infers that the client's data and the tasks related to computing are to be kept secret from CSP and unauthorized users. One of the greatest concerns regarding cloud is confidentiality which is largely due to the loss of physical control. Another concept concerning cloud is data integrity.

In this paper, the concerns based on secure data storage in cloud are addressed. Data centers which are distributed geographically in different locations form the cloud. Data Owners as well as Data Users are not aware where their data is assigned and therefore they have a notion that they have lost authority over their data after it is uploaded to the cloud. Appropriate access control policies and systems are required to allow the Data Owners to control the access to their data stored in cloud. The access policies must restrict data access to only those data users expected by the data owners. These policies need to be imposed by the cloud. In most of the existing cloud storage systems, the cloud service providers are

considered to be trusted by the data owners to restrict the unauthorized data users from making use of their data.

In role-based access control (RBAC) model, access permissions are generalized based on their roles and roles are charted according to the users. In traditional access control systems, trusted parties carry the enforcement which is usually the service providers. In cloud, as the data is saved in distributed data centers, a single central authority might not control all the data centers. Moreover, the cloud service provider administrators themselves would be able to access the data if it is stored in plain format. To protect the privacy of data, data owners apply cryptographic techniques to encrypt the data so that only the data users are granted permissions to access the data as specified by the access policies.. Only the authorized users are able to decrypt the data using their private key after satisfying the access policies and no one else will be able to publish the data content.

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. Data integrity can also be ensured if only authenticated persons can access the cloud services and proper encryption is done while transferring data. Having the best possible authentication mechanism along with a complete security plan can mitigate most of the security concerns of cloud consumers.

This private cloud architecture is used to store not only the organization's complex data but also the actual data that is in the encrypted form. This architecture not only eliminates the organization's concerns related to possible leakage of critical data but also takes full advantage to securely store large volume of data. By making use of these features, the architecture of the proposed system achieves a productive and practical cloud data storage system which is more secure.

Main Contributions: The main contributions of this paper (i) to study the existing approaches of secure data transfer over network in Cloud using proper authentication (ii) to develop an algorithm which securely transfers data over network and provides three way protection in terms of authenticity, integrity and confidentiality (iii) to propose an Admission policy for voting purpose of Data Owners (iv) to develop a Role based access control system for restricting the access of resources to users and (v) To verify and validate the proposed techniques.

The paper is organized as follows: the next Section II presents related work. The proposed architecture of our security solution is presented in Section III which includes the CSP, Data Owner, and Data User. Section IV contains the implementation details. In Section V, the conclusion of our work is presented.

2. RELATED WORK

This literature survey gives a brief introduction to several solutions for authentication, encryption, data access control and also surveys the methods of security and privacy preserving in cloud computing.

Zhifeng Xiao, Yang Xiao [1] consistently studied the security and privacy issues in cloud computing based on an attribute-driven methodology. The authors classified the security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy- preservability) as well as discussed the vulnerabilities, which may be exploited by the attackers to perform various attacks. Defense strategies and their approaches were discussed as well. The authors believe that this analysis will be helpful to shape the future research in the areas of cloud security and privacy. Throughout the study, the authors obtained a common goal to provide an extensive report of the existing security and privacy issues in cloud environments.

Hu Shuijing [2] stated the basic problems arising in the cloud while accessing the data and the security related issues and countermeasures to tackle the problem. Issues like Unwanted Access, data segregation, vendor lock in, data romance, etc are covered in this paper.

B.Rimal [3] surveyed various cloud computing environments and services developed by various projects such as Google, force.com, amazon, open source. The surveyed results are used to identify the similar and different architectural approaches of cloud computing. The author defines the taxonomy and comparative study of cloud computing systems. On the basis of proposed taxonomy and technical studies, the author has evaluated the different cloud computing systems to provide necessary information that can help in future for the new developments and improvement in existing systems. The proposed taxonomy provides researcher and developer the ideas on the current cloud systems, hype and challenges.

Ali A Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou[4] presented an efficient scheme for privacy preserving password authentication for cloud computing. A system to prove the authenticated users identity without the need to admit their passwords is stated in this. The idea of using a Data Owner has been implemented in this paper. Here, in this paper privacy has been the main focus and not security of data.

Nelson Mimura Gonzalez, Marco Antônio Torrez Rojas, Marcos Vinícius Maciel da Silva [5] included solutions to cloud issues from related technologies One of the concerns the authors stated is authentication and authorization in cloud to afford powerful system to identify entities and establish their permissions and roles in the cloud, control the usage of resource and to promote accounting and isolation. They also study the framework related to authorization and authentication including the possible types of credentials, the cloud level of organization level and other requirements such as security, privacy, compliance and lifecycle of the cloud elements.

Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan [6], proposed a semi-anonymous attribute-based privilege control scheme and a fully-anonymous attribute-based privilege control scheme to address the user privacy problem in a cloud storage server. In general, the authorities who are not trusted try to achieve the user attributes to gain access to cloud. Data Consumers are also not to be trusted as they are random users including adversaries. They may also conspire with other Data Consumers to illegally access what they are not allowed to. Here in this paper, the authors concentrated mainly on providing anonymous control for the genuine users.

F. Amounas and E. H. El Kinani [7] presented a work based on the concept of ECC and provided a new method to secure the output of ECC.

V. Gayoso Mart´ınez and L. Hern´andez Encinas [8] facilitated the usage of ECC in Java by analyzing the capabilities and dealing with key generation, key exchange, and digital signatures.

Xin Zhou and Xiaofei Tang [9] proposed an implementation of RSA encryption and decryption solution which is based on the study of RSA public key algorithm.

Access control is one of the significant aspects of network security. Wei Qiu, Carlisle Adams [10], specifies the significant impact of integrity, confidentiality and availability of cloud. They formulated a Role-Based Access Control (RBAC) for approaches based on roles that individual users have as members of a system. In RBAC, there are role hierarchies in which a senior role inherits the permissions of a junior role. Various delegation models have been proposed by the authors in this paper to allow a junior role to perform one or more tasks of a senior role,. In this paper, the authors presented a new role-based delegation model called User-to-Role Delegation Model (URDM), to support multiple delegation, role hierarchy, and single-step delegation.

Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan [11] presented a paper addressing the open challenge problem using capability based access control technique which ensures only valid users to access the outsourced data. In this work, the authors proposed a modified Diffie-Hellman key exchange protocol between cloud service provider and the user to secretly share a symmetric key for secure data access. This also mitigates the problem of key distribution and management at cloud service provider. The idea of using a Data Owner has been implemented in this paper.

Lukas Malina and Jan Hajny [12] presented a unique security solution for privacy-preserving in cloud services. This solution provided anonymous access to users who are registered to cloud services but CSP is given more privileges which is not good regarding the security point of view. Anonymous access phase is successful but focus is on privacy and not on security of data.

As we can see from above related works, the existing user authentication schemes has certain security flaws and concentrates mainly on privacy than security. In this paper, the comparison of these existing schemes can be used to accomplish RBAC policies and Admission Policy in our proposed system.

3. ARCHITECTURE

In this section, the architecture of our secure cloud storage system is presented in Fig 1. It is a private cloud architecture which is used to store the encrypted data of the Data Owners.

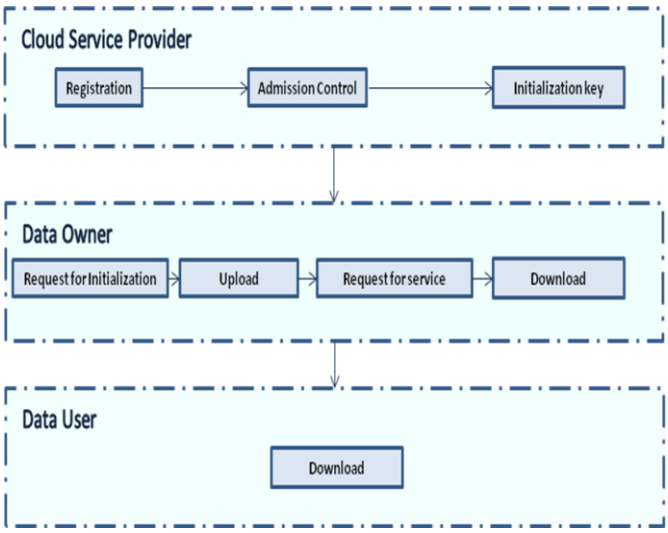

Fig.1: Architecture of the proposed system

In our scheme, plaintext is hidden (i.e. encrypted) in order to provide data protection and privacy preservation. The CSPs

are responsible for data storage, verifying users' ID, and blocking non-eligible users from accessing the data. Secret key issuing is handled by CSP's who acts as a key distribution center to ensure safe data access by trustworthy users. A Data User firstly sends a request to enter the cloud service provider and CSP will check if the user's ID in the system is valid. If it is the case, the CSP will forward the access request to the Data Owner, who will decide if the Data User who sends the request is eligible to access the data. Only with the consent of the Data Owner, the CSP will issue the decryption key to the Data Owner.

3.1 Architectural Components

The components of the system architecture are shown in Fig 1:

Private Cloud: Private cloud [3] is built on an internal data center. The organization itself hosts and operates the data center. The organization stores all the sensitive and confidential information in this private cloud. The amount of the information stored in private cloud is relatively less when compared to the data stored in public cloud. Hence, the private cloud does not need to have huge capacity to handle large volumes of data like the public cloud.

Cloud Service Provider (CSP): CSP offers its customers storage or software services available via a public network or private network.CSP is a company who is partially trusted. Whenever the user accesses the cloud service, the CSP validates the user and issues access attributes to users. The CSP also acts as the key distribution center.

Data Owner (DO): DO [4] is a cloud client who registers with the CSP.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

Data User (DU): DU is a cloud client who registers with the CSP. Whenever a DU query for data to the CSP, the CSP provides a list of DO who possesses the data. DU is also anonymous if they follow the rules of the CSP accordingly.

3.2 System Operations

In this section, the system operations of our proposed architecture are described:

Registration: In the registration phase [5], the new Data Owner registers himself in order to upload and view his files. In the process of registration, the new Data Owner sends its request to the CSP giving necessary details such as user id, password, first name, last name, and email id. Once the CSP acquires the request for registration from the new Data Owner, the CSP posts the new Data Owner details to the existing Data Owner's for feedback. The registration process of Data User is same as that of the Data Owner except for the voting part.

Admission Control Policy: In this phase, the new Data Owner to get access to the cloud must be accepted by the CSP. For this, the CSP depends on the feedback given by the existing Data Owner's which is carried out by voting process. Once a new Data Owner gets minimum number of votes (i.e. greater than or equal to 50% of votes from the existing Data Owners) then only the CSP accepts the new Data Owner.

Initialization: Once the registration is successful with the CSP i.e. the CSP accepts the new Data Owner, the DO has to go through the next level of security. Once this is done, an initialization key is sent to the DO/DU in their registered email id. After the initialization phase the DO/DU has to answer two security questions. The DO/DU can now start communication process with the CSP. Whenever the DO/DU wants to communicate with the CSP they need to enter the initialization key along with the security answers to proceed forward. Without any one of the details, the DO/DU cannot proceed with any services on the cloud.

Anonymous Communication: After the initialization phase is successful, the DO/DU can access the cloud anonymously [6] i.e. which DO or DU is exchanging the data between themselves is not revealed. Their identities are hidden.

Admission Control – Request for registration: When a new Data Owner wants to register to cloud, he/she should make a registration request to cloud. Once the CSP receives a registration request from the new Data Owner, the CSP sends the list of new data owner's to be registered to the existing data owner's.

Admission Control – Voting for new Data Owner: The Data Owners sends a feedback to the CSP. Once the new Data Owner is accepted, accordingly as per the admission control policy the CSP registers the new data owner and sends the initialization key to the new Data Owner.

Access control-Upload data: The encrypted data is uploaded to the cloud by the Data Owner. The DO can encrypt the file using either RSA or ECC encryption technique. The choice of encryption is of the DO. The RSA and ECC encryption algorithms are given below in detail.

Access Control – Request to access Data (services): The Data Owner/Data User has to send a request to the respected Data Owner to access [10][11] any data. Now, the Data Owner will decide if he/she wants to share the data with the Data User or not. If the Data Owner wishes to share his data, he/she will give permission to the CSP to send the decryption key to the Data Owner/Data User's registered email id.

Access Control – Download Data: If the Data Owner wants to download a particular file, then he/she would communicate with the CSP to provide the list of DO who has the data. The DO sends a request to the concerned Data Owner. Once the

CSP send the decryption key to DO, he/she can download the concerned data.

Access Control – Download Data (Data User): The Data User is provided with Role-based Access Control (RBAC) policy. In our proposed system, the privileges of the Data User are reduced and the DU can only download data from the cloud. In the proposed system, to protect the sensitive information the Data Owner specifies their own access privacy policies. Access can be restricted to certain information. Apart from this, it also helps the customer to increase his confidence and provides continuous data access with the touch of a button from anywhere at any time.

3.3 Cryptography Used

Encryption algorithms are mainly used to keep the data safe from any kind of attack. The best and the most efficient algorithms have to be used since the data is stored in a third party data center and also large amounts of data transfer takes place during this process. Here, in this proposed solution, the Data Owner can choose any of the public-key encryption algorithms i.e. ECC or RSA [7][8][9] to encrypt their data.

RSA algorithm is based on the difficulty of factoring large integers [6]. RSA user creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of prime factors can possibly decode the message. The decryption of RSA cipher text is infeasible as there is no efficient algorithm for integer factorization.

Elliptic Curve Cryptography (ECC) relies on the algebraic structure of elliptic curves over finite fields [4] [5]. It is assumed that identifying the discrete logarithm of a random elliptic curve element in connection to a publicly known base point is impractical. The advantage of the ECC algorithm over RSA is that the key can be smaller, resulting in improved speed and security.

Here, for this system, the key size for ECC is 160 bits and RSA is 1024 bits.

4. IMPLEMENTATION

We have implemented the above architecture of the secure cloud data storage system. The system is implemented in Java. The DO and DU communicate with the help of web interface and uses personal computer, laptop, tablet or a smart phone for communication. Our solution is tested on a machine with Intel$^{(R)}$ Core i3 processor @ 2.53GHz, 2 GB Ram. In Table 1, an analysis based on load on the CSP is shown. The table compares how the load on the CSP affects with the presence of Data Owner and without the Data Owner.

Operations	**Load on CSP with Data Owner**	**Load on CSP without Data Owner**
1. New Owner Admission	Every registration about new owner is broadcast to the existing DO's to vote for getting initialization keys by CSP. In this process, the load of the CSP is shared by the DO.	Every New Users services are directly depended on the CSP. CSP does not test the authenticity and gives initialization keys at random. The CSP has to take the complete load of registration process.
2.Download Service	DU has to take permission from the DO only. DO has to verify the user and decide to give the services. Then the CSP gives the key to DU to download the file. DO share the load of CSP.	DU has to take permission i.e. keys from the CSP only. User verification task also done by CSP. Complete load on CSP
3. Performance w.r.t. New Data Owner Admission	CSP has to wait for acceptance which delays the process of admission.	CSP can directly give initialization keys to New Data Owner as no restriction is there. So it will take less time for admission process.
4. Performance of System	System performance is positively affected by the inclusion of Data Owner. Again Data Owner has to share a load of CSP i.e. central server as Owner has to handle request from the Data User.	System performance of CSP lowers as the CSP has to do all the tasks like admission control, anonymous access, as well as handle the Data User request.

Table 1: Analysis based on Load on CSP

From the table, we can see that the load on the CSP is considerably reduced with the inclusion of Data Owner as the Data Owner shares some of the responsibilities of the CSP.

5. CONCLUSION

Cloud is a promising and emerging technology for the next generation of IT applications. The drawback towards the accelerated growth of cloud computing is data security and privacy issues. Researchers have proposed a number of techniques for data protection and to achieve higher levels of data security in the cloud. There are systems which allow authenticated users to communicate with each other in an encrypted form. Those systems offer strong encryption and confidentiality through authenticated users but they do not focus on anonymous authentication. There may be systems which provides anonymous access to users but do not focus on confidentiality. Our solution combines an anonymous authentication for a registered user along with ECC, RSA encryption techniques and also provides confidentiality and integrity where the cloud clients can send encrypted messages to each other. Traditional access control techniques which have been developed for Cloud environment do not support both i.e. privacy and security issues in cloud. For enhancing privacy along with security in the cloud, Role Based Access Control technique is proposed in this work.

For secure cloud environment, the following methods were proposed to protect user's privacy and security of data: (1) Two-tier authentication to protect the confidentiality of the Data owner and Data User (2) deploying an admission control policy to provide feedback voting for new Data Owner (3) storing the data after encryption (4) RBAC policy to control the usage of Data Owner's data.

This solution provides a good secure and anonymous communication system for all users. The focus is on data storage and data protection in the cloud environment, to build trust, confidence between cloud service providers and consumers. Yet, there are many gaps to be filled by making these techniques more efficient. More work is required to be carried in the area of cloud computing and to make it suitable for the cloud service consumers.

REFERENCES

[1] Zhifeng Xiao,Yang Xiao,"Security & Privacy in Cloud Computing", IEEE,2013.
[2] Hu Shuijing," Data security: The challenges of Cloud Computing",IEEE, 2014.
[3] B.Rimal et al., "A Taxonomy and Survey of Cloud Computing Systems", International Joint Conference on INC, IMS and IDC, 2009.
[4] Ali A Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou," A Practical Privacy- preserving Password Authentication Scheme for Cloud", IEEE,2012.
[5] Nelson Mimura Gonzalez, Marco Antônio Torrez Rojas, Marcos Vinícius Maciel da Silva, "A framework for authentication and authorization credentials in cloud computing", IEEE, 2013.
[6] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan," Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption",IEEE, 2015.
[7] F. Amounas and E. H. El Kinani," ECC Encryption and Decryption with a Data Sequence", Applied Mathematical Sciences, 2012.
[8] V. Gayoso Mart´ınez and L. Hern´andez Encinas, "Implementing ECC with Java Standard Edition 7", International Journal of Computer Science and Artificial Intelligence, 2013.
[9] Xin Zhou,Xiaofei Tang, "Research and Implementation of RSA algorithm for Encryption and Decryption", IEEE,2011.
[10] Wei Qiu, Carlisle Adams," Exploring User-to-Role Delegation in Role-Based Access Control", IEEE, 2007.
[11] Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan, "Secure Data Access in Cloud Computing", IEEE,2010.
[12] Lukas Malina, Jan Hajny, "Efficient Security Solution for Privacy-Preserving Cloud Services", IEEE, 2013
[13] Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang," Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE, 2015.
[14] Peter Mell, Tim Grance, "The National Institute of Standards and Technology (NIST), Information Technology Laboratory definition of Cloud Computing", Version 15, 2009.
[15] Divya Pritam, Madhumita Chatterjee, "Privacy-Preserving in Cloud Computing with Security-as-a-Service", IJRITCC, Vol.3, 2015.

Authors

Divya Pritam has completed her Bachelor's Degree from Jawaharlal Nehru Technological University, Andhra Pradesh, and doing her Master's Degree at Pillai Institute of Information Technology, Mumbai University. She is having 1 year of experience in teaching field. Her area of interest is in Networking and Security. Her Master's thesis is focused on Privacy-Preserving in Cloud Computing with Security-as-a-Service, doing under Dr. Madhumita Chattejee who has completed her PhD degree from IIT, Mumbai.

Dr. Madhumita Chatterjee has completed her PhD from IIT, Mumbai. She is now working as HOD of Computer Engineering Department at Pillai Institute of Information Technology, Navi Mumbai, Maharashtra. She is having over 20 years of teaching experience and provides valuable guidance to her students in many research areas like Network Security, Cyber Security. She has conducted many workshops on Network Security and also worked as a coordinator for workshops conducted by IIT, Mumbai.