International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

# A Data Centric Access Control Solution with Role Based Expressiveness for Protecting User Data on Cloud

**P Manjunatha[1], Mrs. Roopa B K[2], Dr. Kavitha K S[3], Dr. Kavitha C [4]**

*[1]PG Student, Department of CSE, Global Academy Of Technology, Bengaluru, Karnataka, India*
*[2]Associate Professor, Department of CSE, Global Academy Of Technology, Bengaluru, Karnataka, India*
*[3]Professor, Department of CSE, Global Academy Of Technology, Bengaluru, Karnataka, India*
*[4]Professor & HOD, Department of CSE, Global Academy Of Technology, Bengaluru, Karnataka, India*

---

**Abstract -** *Most current security solutions are primarily based on perimeter protection. But, Cloud computing breaks the organization perimeters. Along with data residing within the Cloud, they also reside outside the organizational bounds. This will make users to lose control over their data and will increase security issues that slow down the use of Cloud computing. Is the Cloud service provider having access to the data? Is it using the access control policy defined by the user? This paper gives a Data-Centric access control answer with enriched function primarily based expressiveness in which safety is the main target on protecting person records regardless the cloud carrier company that holds it. Novel identity based and proxy re-encryption strategies are used to protect the authorization model. Data is encrypted and authorization regulations are cryptographically covered to keep user statistics in the direction of the service provider access or misbehavior. The authorization model offers high expressiveness with role hierarchy and resource hierarchy support. The solution takes benefit of the logic formalism provided through Semantic web technologies, which enables superior rule management like semantic conflict detection. An evidence of concept implementation has been evolved and a working prototypical deployment of the proposal has been integrated inside Google services.*

***Key Words*: *Data-centric security, Cloud computing, Role-based access control, Authorization.***

## 1. INTRODUCTION

Security is one of the primary user concerns for the adoption of Cloud computing. Transferring data to the Cloud usually implies relying on the Cloud Service Provider for data protection. Even though that is generally controlled based on legal or service level Agreements (SLA), the CSP should potentially access the data or maybe offer it to third parties. Furthermore, one need to agree with the CSP to legitimately apply the access control rules defined by means of the data owner for other users. The problem becomes even more complex in Inter-cloud scenarios in which data can also flow from one CSP to some other. Users might also lose control on their data. Even the agree with at the federated CSPs is outside the control of the data owner. This case results in rethink about data security methods and to transport to a data-centric method where data are self-protected every time they reside.

Encryption is the most widely used method to protect data in the Cloud. In reality, the Cloud security Alliance protection guidance recommends information to be included at relaxation, in movement and in use [1]. Encrypting information avoids undesired accesses. However, it involves new problems associated with access control management. A rule-based approach could be ideal to offer expressiveness. However this poses a huge challenge for a data-centric method considering the facts that have no computation abilities by way of itself. It is not able to put in force or compute any access control rule or policy. This increases the difficulty of policy selection for a self-included information package: who need to evaluate the guidelines upon an access request? The first preference would be to have them evaluated by using the CSP, but it is able to potentially pass the guidelines. Some other choice would be to have guidelines evaluated via the information owner, however this implies that either information could not be shared or the proprietor need to be on-line to take a choice for each access request.

To overcome the aforementioned issues, several proposals [2] [3] [4] try to provide data-centric solutions based on novel cryptographic mechanisms applying Attribute based Encryption (ABE) [5]. These solutions are based on Attribute-based Access Control (ABAC) [16], in which privileges are granted to users according to a set of attributes. There is a long standing debate in the IT community about whether Role-based Access Control (RBAC) [6] or ABAC is a better model for authorization [7] [8] [9]. Without getting into this debate, both methods have their very own pros and cons.

To the best of our information, there may be no data-centric method imparting an RBAC (role based access control) version for access control in which data is encrypted and self-covered. The proposal on this undertaking supposes a first answer for a data-centric RBAC approach, providing an opportunity to the ABAC model. An RBAC (attribute based access control) technique might be in the direction of modern access control strategies, ensuing extra natural to apply for access control enforcement than ABE-primarily

based mechanisms. In terms of expressiveness, it's far stated that ABAC supersedes RBAC due to the fact that roles may be represented as attributes. But, in terms of data-centric approaches in which data is encrypted, ABAC solutions are restricted by the expressiveness of ABE schemes. The cryptographic operations utilized in ABE typically limit the level of expressiveness for access control policies. As an instance, function hierarchy and item hierarchy abilities can't be done by way of current ABE schemes. Furthermore, they usually lack a few mixtures with a person-centric approach for the access control policy, where common authorization-associated factors like definition of customers or role assignments might be shared via distinct pieces of facts from the identical data owner.

This paper presents SecRBAC, a data-centric access control solution for self-protected data that can run in untrusted CSPs and provides extended Role-Based Access Control expressiveness. The proposed authorization solution provides a rule-based approach following the RBAC scheme. This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing. Role hierarchies and resource hierarchies are supported by the authorization model, providing more expressiveness to the rules by enabling the definition of simple but powerful rules that apply to several users and resources thanks to privilege propagation through roles and hierarchies. Policy rule specifications are based on Semantic Web technologies that enable enriched rule definitions and advanced policy management features like conflict detection. A data-centric approach is used for data protection, where ideal cryptographic techniques such as Proxy Re-Encryption (PRE) [10], Identity Based Encryption (IBE) [11] and Identity-Based Proxy Re-Encryption (IBPRE) [12] are used. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. These techniques are used to protect both the data and the authorization model. Every data is encrypted with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also merges a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data. The solution enables a rule based approach for authorization in Cloud systems [13] [14] where rules controlled by the data owner and access control computation is handed over to the CSP, but making it unable to grant access to unauthorized parties.

Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These new creative, technical and costing opportunities bring changes in the way business operated. Cloud computing is the matchless computing technology. Cloud computing is a new label to an old idea. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing allows for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. General example of cloud services are Google Engine, Oracle Cloud, Office 365. As the cloud computing is growing rapidly this also leads to severe security facts. Insecurity is the only barrier in wide adoption of cloud computing. The fast growth of cloud computing has brought many challenges for users and providers.

## 1.1 Cloud Security Issues

While cost and ease of use are the two main strong benefits of the cloud computing, there are some major alarming issues that need to be referenced when allowing moving critical application and sensitive information to cloud(both public as well as shared).

### 1.1.1 Data confidentiality issue:

Confidentiality is a set of rules or an agreement that bounds access or location restriction on certain types of information so in cloud data reside publically so Confidentiality refers to, customer's data and computation task are to be kept confidential from both cloud provider and other customers who is using the service. We must make sure that user's private or confidential information should not be accessed by anyone in the cloud computing system, including application, platform, CPU and physical memory. It is clear that user's confidential data is disclosed to service provider on the following situation only.

### 1.1.2 Data availability issue:

When keeping data at remote location which is owned by others, data owner may face the problem of system failure of the service provider. And if cloud stops working, data will not be available as the data depends on single service provider. Challenges to data availability are flooding attacks causes deny of service and Direct /Indirect (DOS) attack. Cloud computing is to provide on-demand service of different levels. If a particular service is not available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose trust.

### 1.1.3 Data integrity issue:

As the word itself explains the "completeness" and "wholeness" of the data which is the basic and central needs of the information technology, As we know that integrity of data is important in the database equally integrity of data storage is important and necessary requirement in the cloud, it is the key factor that changes the performance of the cloud. The data integrity proofs the validity, consistency and regularity of the data. It is the perfect method of writing of the data in a secure way the persistent data storage which can be reclaim or retrieved in the same layout as it was stored later. Therefore cloud storage is becoming popular for

the outsourcing of day-to-day management of data .So integrity monitoring of the data in the cloud is also very important to escape all possibilities of data corruption and data crash. The cloud provider should provide surety to the user that integrity of their data is maintained in the cloud.

## 2. LITERATURE REVIEW

Different approaches can be found in the literature to retain control over authorization in Cloud computing. In some paper, authors propose to keep the authorization decisions taken by the data owner. The access model is not published to the Cloud but kept secure on the data owner premises. However, in this approach the CSP becomes a mere storage system and the data owner should be online to process access requests from users. Another approach for dealing with this issue is by enabling a plug-in mechanism in the CSP that allows data owners to deploy their own security modules.

This permits to control the authorization mechanisms used within a CSP. However, it does not establish how the authorization model should be protected, so the CSP could potentially infer information and access the data. Moreover, this approach does not cover Inter-cloud scenarios, since the plug-in module should be deployed to different CSPs. Additionally, these approaches do not protect data with encryption methods. In the proposed SecRBAC solution, data encryption is used to prevent the CSP to access the data or to release it bypassing the authorization mechanism.

However, applying data encryption implies additional challenges related to authorization expressiveness. Following a straightforward approach, one can include data in a package encrypted for the intended users. This is usually ensures that the only receiver who has an appropriate key can decrypt it and is done when sending a file or document to a specific receiver.

From an authorization view, this can be a simple rule where only the user with access privilege to data will be able to decrypt it. However, access control expressiveness is not provided by this approach. Only that simple rule can be enforced and just one single rule can apply to each data package. Thus, multiple encrypted copies should be created in order to deliver the same data to different receivers.

To cope with these issues, SecRBAC follows a data-centric approach that is able to cryptographically protect the data while providing access control capabilities. Many data-centric methods, mostly based on Attribute- based Encryption (ABE) [15], have arisen for data protection in the Cloud. In ABE, the encrypted ciphertext is labeled with a set of attributes by the data owner. Users also have a set of attributes defined in their private keys. They would be able to access data (i.e. decrypt it) or not depending on the match between ciphertext and key attributes.

The set of attributes needed by a user to decrypt the data is defined by an access structure, which is specified as a tree with AND and OR nodes. There are two main approaches for ABE depending on where the access structure resides: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE the access structure or policy is defined within the private keys of users. This allows encrypting data labeled with attributes and then controlling the access to such data by delivering the appropriate keys to users. However, in this case the policy is really defined by the key issuer instead of the person who encrypts the data, i.e. the data owner. So, the data owner should trust the key issuer for this to properly generate an adequate access policy. To solve this issue, CP-ABE proposes to include the access structure within the ciphertext, which is under control of the data owner.

In SecRBAC, user keys only identify their holders and they are not tied to the authorization model. That is, user privileges are completely independent of their private key. Finally, user-centric approach for authorization rules is not provided by current ABE solutions. In SecRBAC, a single access policy defined by the data owner is able to protect more than one piece of data, which results in a user-centric method for rule management. Additionally, the proposed solution provides support for the ontological representation of the authorization model [14], providing additional reasoning mechanisms to cope with issues such as detection of conflicts between different authorization rules.

## 3. SYSTEM ARCHITECTURE

The design of the system is perhaps the most critical factor affecting the quality of the software. The objective of the design phase is to produce overall design of the software. It aims to figure out the modules that should be in the system to fulfill all the system requirements in an efficient manner.

The design will contain the specification of all these modules, their conversation with other modules and the required output from each module. The output of the design process is a description of the software architecture. Three major divisions in this project are:

### 3.1 Data Access Layer

Data access layer is the one which exposes all the possible operations on the data base to the outside world. It will contain the DAO classes, DAO interfaces, POJOs, and Utils as the internal components. All the other modules of this project will be communicating with the DAO layer for their data access needs.

### 3.2 Account Operations

Account operations module provides the following functionalities to the end users of our project.

- Register a new seller/ buyer account
- Login to an existing account
- Logout from the session
- Edit the existing Profile
- Change Password for security issues
- Forgot Password and receive the current password over an email
- Delete an existing Account

Account operations module will be re-using the DAO layer to provide the above functionalities.

### 3.3 Authorization Rules

Authorization rules is a collection of tuples, where each tuple will have a role name along with the type of access granted to that role. For instance, Role name can be a DOCTOR, TEACHER, STUDENT, AUTHOR, etc., and then the type of access can be READ ONLY ACCESS, READ WRITE ACCESS, etc. An end user of this project can create any number of authorization rule with any number of tuples within it. The user can manage all his/her authorization rules at any time by adding a new rule or by removing the existing rule. The authorization rule created in this module will be used in the manage data module for mapping the user data with the appropriate rule.

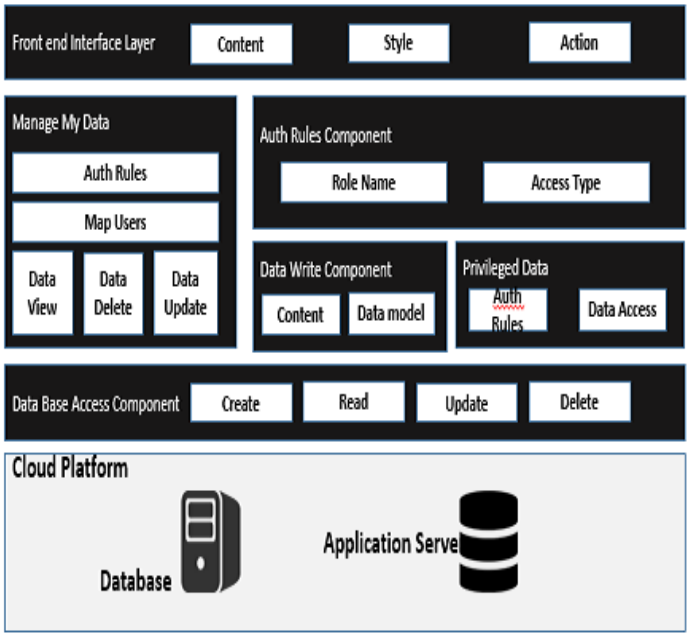


**Fig -1:** Proposed System Architecture

### 3.4 Manage Data

Here, the user of this project will be able to perform various operations on his/her data. The operations include data write, data read, data update, and data delete. The user upon writing a new data will be performing the cryptographic operation on their data thus encrypting the data before uploading it to the cloud. The user will also be able to perform other operations like mapping the data with the appropriate authorization rule created in the previous module, and also he/she can perform mapping the user to appropriate role of the defined authorization rule.

### 3.5 Privileged Data Access

Here, the end user of this project can access the data uploaded by the other users of this project if they have granted the access to this logged in user. The user will be mapped to appropriate role of the authorization rule and they will be able to access the data as per the access policy defined by the rule. For accessing the data, the user will be have provide his identity (which can be his email id, phone number, pan number etc.) upon which an email will be sent to him/her after which our project will execute the double encryption algorithm to grant access on this data to that user.

Fig-1 shows the above 5 modules implemented in the form of Architecture.

## 4. CONCLUSIONS

A data-centric authorization solution has been proposed for imparting security to the data in cloud. SecRBAC manages authorization via following a rule-based approach and provides role-based expressiveness consisting of role hierarchies and item hierarchies. Access control calculations are transferred to the CSP. Latest cryptographic techniques have been implemented to secure the authorization model. A key for re-encrypting enhances every authorization rule as cryptographic token to defend data against CSP misbehavior. The solution is unbiased of any PRE scheme or implementation as far as 3 specific features are supported. The IBPRE scheme has been used in this paper so that it will offer a complete and feasible solution.

A proposal based on Semantic Web technologies has been exposed for the representation and evaluation of the authorization technique. It also makes use of the semantic techniques of ontologies and the computational abilities of reasoners to mention and test the model. This also enables the application of advanced techniques such as conflict detection and resolution techniques. Guidelines for deploying in a Cloud Service Provider have also been given, that includes a hybrid method which is compatible with Public Key Cryptography that enables the usage of standard PKI for key management and distribution. A prototypical

method is implemented which been also developed and exposed in this paper, with some results of the experimentation.

## 5. FUTURE WORK

Future lines of research include the analysis of novel cryptographic techniques that could enable the secure modification and deletion of data which is in the Cloud. This would give permission to extend the privileges of the authorization model with more actions like edit and delete. Another important point is the obfuscation of the authorization model for privacy motives. Although the usage of pseudonyms is already proposed, a more advanced obfuscation methods can be found to achieve a higher level of privacy.

## REFERENCES

[1] Cloud Security Alliance, "Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0," CSA, Tech. Rep., 2003.

[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, "Feacs: A Flexible And Efficient Access Control Scheme For Cloud Computing," in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.

[3] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[4] B. B and V. P, "Extensive Survey on Usage Of Attribute Based Encryption In Cloud," Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption For Fine-Grained Access Control Of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, 2006, pp. 89–98.

[6] Inter National Committee for Information Technology Standards, "INCITS 494-2012 - Information Technology – Role Based Access Control - Policy Enhanced," INCITS, Standard, Jul. 2012.

[7] E. Coyne and T. R. Weil, "Abac and Rbac: Scalable, Flexible, and Auditable Access Management," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[8] Empower ID, "Best Practices in Enterprise Authorization: The RBAC/ABAC Hybrid Approach," Empower ID, White paper, 2013.

[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding Attributes To Role Based Access Control," Computer, vol. 43, no. 6, pp. 79–81, 2010.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes With Applications To Secure Distributed Storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.

[11] F. Wang, Z. Liu, and C. Wang, "Full Secure Identity-Based Encryption Scheme with Short Public Key Size Over Lattices In The Standard Model," Intl. Journal of Computer Mathematics, pp. 1–10, 2015.

[12] M. Green and G. Ateniese, "Identity-Based Proxy Re-Encryption," in Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ser. ACNS '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 288–306.

[13] A. Lawall, D. Reichelt, and T. Schaller, "Resource Management and Authorization for Cloud Services," in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1–18:8.

[14] D. Y. Chang, M. Benantar, J. Y.-c. Chang and V. Venkataramappa, "Authentication and Authorization Methods for Cloud Computing Platform Security," Jan. 1 2015, us Patent 20,150,007,274.