International Journal of Computational Research and Development (IJCRD)
Impact Factor: 4.775, ISSN (Online): 2456 - 3137
(www.dvpublication.com) Volume 1, Issue 2, 2016

ROLE BASED SECURED ACCESS OF DATA IN CLOUDS

R. Saravana Kumar* & Dr. P. Suresh**
* M.Tech-Information and Cyber Warfare, Department of Information Technology, Kongu Engineering College, Perundurai, Tamilnadu
** Assistant Professor, Department of Information Technology, Kongu Engineering College, Perundurai, Tamilnadu

Cite This Article: R. Saravana Kumar & Dr. P. Suresh, "Role Based Secured Access of Data in Clouds", International Journal of Computational Research and Development, Volume 1, Issue 2, Page Number 76-82, 2016.

Abstract:

In mobile wireless sensor network, coverage and energyCloud computing is a type of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources e.g., computer networks, servers, storage, applications and services, which can be rapidly provisioned and released with minimal management effort. Attribute-based access control defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes such as user attributes, resource attributes, object and environment attributes etc. This model supports Boolean logic, in which rules contain "if-then" statements about who is making the request, the resource and the action. The main problem in attribute–based access control is not having user-centric approach for authorization rules. In ABAC model role hierarchy and object hierarchy is not achieved and restriction in level of expressiveness in access control rules.Secured role-based access control allows managing authorization based on rule-based approach where rules are under the control of data owner and provides enriched role-based expressiveness including role and object hierarchies. Data user without the knowledge of data owner cannot use the cloud server where privilege is provided to data user by data owner. Access control computations are delegated to the cloud service provider, being this not only unable to access the data, but also unable to release it to unauthorized parties. A identity-based proxy re-encryption scheme has been used in order to provide a comprehensive and feasible solution for data centric-approach. Semantic web technologies have been exposed for the representation and evaluation of the authorization model.

Key Words: Data-Centric Security, Cloud Computing, Role-Based Access Control & Authorization

1. Introduction:

In Cloud Computing is the use of hardware and software to deliver a service over a network (typically the internet). With cloud computing, users can access files and use applications from any device that can access the internet. An example of a cloud computing provider is Google's Gmail. Cloud computing is a type of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Cloud computing is aimed at providing IT as a service to the cloud users on-demand basis with greater exibility, availability, reliability and scalability with utility computing model.Every user is assigned a role, and each role is assigned specific level of access privilege that are inherited by the user.A data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user dataregardless the Cloudservice provider that holds it.Authorizing an user to access the with prior permission from the user and access of resources with user permission. They can aid administrators with this task by enabling the specification of highlevel access control rules that are automatically interpreted by system for this to behave as defined by the administrator. RBAC is an authorization scheme supported by most of the current authorization solutions. Data centric security is an approach to security that emphasises the security of data itself rather then security of the network. The Ontology Web Language (OWL) is a family of knowledge representation languages for authoring ontologies. Ontologies are a formal way to describe taxonomies and classification networks, essentially defining the structure of knowledge for various domains: the nouns representing classes of objects and the verbs representing relations between the objects. The OWL languages are characterized by formal semantics. They are built upon a W3CXML standard for objects called the Resource Description Framework (RDF).

2. Motivation of Our Work:

In the existing system ABAC model is used for secure access of data in clouds. ABAC in which privileges are granted to users according to a set of attributes.To provide data centric solution based on novel cryptographic mechanisms provide attribute based encryption. In ABAC, if a user has attributes that are reflected in the objects they want to access, then access is granted. In ABAC permissions can be acquired dynamically by virtue of the user's attributes.To achieve this granularity of access in ABAC requires rule sets that apply when attributes are evaluated. Different approaches can be found in the literature to retaincontrol over authorization in Cloud computing. In [13] 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 from [14] deals with this issue 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 withencryption methods. In the proposed Sec RBAC solution, data encryption is used to prevent the CSP to access the dataor to release it bypassing the authorization mechanism.However, applying data encryption implies additionalchallenges related to authorization expressiveness. Followinga straightforward approach, one can include data in apackage encrypted for the intended users. This is usuallydone when sending a file or document to a specific receiverand ensures that only the receiver with the appropriate keyable to decrypt it. From an authorization point of view, this can be seen as a simple rule where only the user with privilege access the data will be able to decrypt it (i.e. the one own inthe key). However, no access control expressiveness is 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 createdin order to deliver the same data to different receivers. To cope with these issues, Sec RBAC follows a data-centric approach that is able cryptographically protect the data while providing access control capabilities.Several data-centric approaches, mostly based on Attribute-based Encryption (ABE) [5], have arisen for data protectionin the Cloud [4]. In ABE, the encrypted ciphertext islabeled with a set of attributes by the data owner. Users alsohave a set of attributes defined in their private keys. Theywould be able to access data (i.e. decrypt it) or not dependingon the match between cipher text and key attributes. Theset of attributes needed by a user to decrypt the data isdefined by an access structure, which is specified as a tree with AND and OR nodes. There are two main approachesfor ABE depending on where the access structure resides:Key-Policy ABE (KP-ABE) [5] and Ciphertext-Policy ABE(CP-ABE) [3]. In KP-ABE the access structure or policy isdefined within the private keys of users. This allows to encrypt data labeled with attribute and then control theaccess to such data by delivering the appropriate keys tousers. However, in this case the policy is really defined bythe key issuer instead of the encrypt or of data, i.e. the dataowner. So, the data owner should trust the key issue forthis to properly generate an adequate access policy. To solvethis issue, CP-ABE proposes to include the access structurewithin the cipher text, which is under control of the dataowner. Then, the key issuer just asserts the attributes ofusers by including them in private keys. However, either inKP-ABE or CP-ABE, the expressiveness of the access controlpolicy is limited to combinations of AND and OR attributes. The data-centric solution presented in this papergoes a step forward in terms of expressiveness, providing arule-based approach following the RBAC scheme that is nottied to the limitations of current ABE approaches.Yu Zhang and Jing Cheno (2014) guarantee the confidentiality and security of data sharing in cloud environment, Flexible and Efficient Access Control Scheme (FEACS) is based on attribute-based encryption, which is suitable for fine-grained access control. we prove in the standard model that FEACS is secure based on the Decisional Bilinear Diffie-Hellman assumption. But using this encryption technique cannot able to represent the expressiveness. Hui Ma and Rui Zhang (2015) has two cipher text-policy attribute-based key encapsulation mechanism schemes that for the first time achieve both outsourced encryption and outsourced decryption in two system storage models and give corresponding security analysis. In these schemes, heavy computations are outsourced to Encryption Service Providers (ESPs) or Decryption Service Providers (DSPs), leaving only one modular exponentiation computation for the sender or the receiver. Moreover, use a general verification mechanism for a wide class of cipher text-policy AB-KEM schemes, which can check the correctness of the decryption efficiently. Concretely, we introduce a stronger version of verifiability. Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2012) Hierarchical Attribute-Set-Based Encryption (HASBE) by extending cipher text-policy Attribute-Set-Based Encryption (ASBE) with a hierarchical structure of users. This scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. It formally prove the security of HASBE based on security of the cipher text-policy attribute-based encryption (CP-ABE) scheme by Bethencourt et al. Brent Waters (2012) proposed a new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and no interactive cryptographic assumptions in the standard model. This solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. Atribute-based encryption which used for data-self protection where representation of authorization model is using the encryption technique.

3. Authors Contribution:

Sec RBAC, a data-centric access controlsolution for self-protected data that can run in untrustedCSPs and provides extended Role-Based Access Controlexpressiveness. The proposed authorization solution providesa rule-based approach following the RBAC scheme, where roles are used to ease the management of accessto the resources. This approach can help to control andmanage security and to deal with the complexity of managingaccess control in Cloud computing. Role and resource hierarchies are supported by the authorization model, providingmore expressiveness to the rules by enabling thedefinition of simple but powerful rules that

apply to severalusers and resources thanks to privilege propagationthrough roles and hierarchies. Policy rule specifications arebased on Semantic Web technologies that enable enrichedrule definitions and advanced policy management featureslike conflict detection. A data-centric approach is used fordata self-protection, where novel cryptograhpic techniques such as Proxy ReEncryption (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 touse identities in cryptographic operations. These techniquesare used to protect both the data and the authorizationmodel. Each piece of data is ciphered with its own encryptionkey linked to the authorization model and rulesare cryptographically protected to preserve data against theservice provider access or misbehavior when evaluating therules. It also combines a user-centric approach for authorizationrules, where the data owner can define a unified accesscontrol policy for his data. The solution enables a rulebasedapproach for authorization in Cloud systems whererules are under control of the data owner and access controlcomputation is delegated to the CSP, but making it unableto grant access to unauthorized parties.The main contributions of the proposed solution are:

- ✓ Data-centric solution with data protection for theCloud Service Provider to be unable to access it.
- ✓ Rule-based approach for authorization where rulesare under control of the data owner.
- ✓ High expressiveness for authorization rules applyingthe RBAC scheme with role hierarchy and resourcehierarchy (Hierarchical RBAC or hRBAC).
- ✓ Access control computation delegated to the CSP, butbeing unable to grant access to unauthorized parties.
- ✓ Secure key distribution mechanism and PKI compatibility

4. Proposed Method:

Assumptions: Data-centric role-based access control approach, offering an alternative to the attribute-based access control model. Sec RBAC 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, where roles are used to ease the management of access to the resources. This approach can help to control and manage security and to deal with the complexity of managing access control in cloud computing. 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 self-protection, where novel cryptographic techniques such as Proxy Re-Encryption Identity- Based Encryption and Identity-Based Proxy Re-Encryption 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.

System Model:

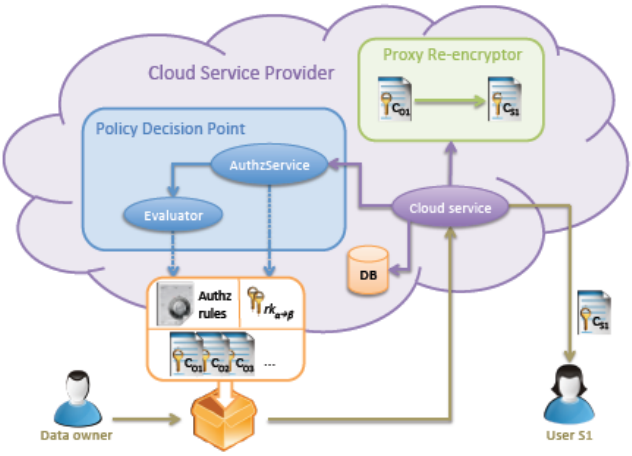

Figure 1: Architecture of System Model

Initialization of Cloud Server Setup: Initialize cloud server setup by connection set up of cloud service provider, data consumer, data owner and authorized service. Using client and server communication we initialize the interface between the cloud service provider and the user.

Authorization Model: The Authorization models with enriched role-based access control expressiveness can help to control and manage security and to deal with this complexity. Authorization model determines privileges that are granted to subjects, RBAC is an authorization scheme supported by most of the current authorization solutions. In this approach, the authorization model makes use of the role concept to assign privileges to subjects. A set of subjects can be assigned to one or more roles which, in turn, can be associated to a set of privileges. This provides more expressiveness to the authorization model, making it easier to manage privilege assignments through roles.

Protecting Authorization Model: A self-protection mechanism is provided to assure data can only be accessed by authorized subjects according to the data owner rules. It is achieved by the application of the cryptographic techniques data-centric security approach data should be encrypted to avoid undesired access. Then, the access control mechanism should control who will be able to decrypt the data and get access to its content. In terms of authorization, this means that the set of objects (O) should be encrypted before being uploaded to the cloud. Moreover, the set of actions (A) is formed by the access action, meaning being able to decrypt the data and get access.

Proxy Re-Encryption: A PRE scheme is a cryptographic scheme that enables an entity called proxy to re-encrypt data from one key to another without being able to decrypt it. That is, given a couple of key pairs and the proxy could re-encrypt a cipher text encrypted under public key to another cipher text that can be decrypted using private key. Using this kind of cryptography, a user (u) can encrypt a piece of data (m) using his own public key (pub) to obtain a cipher text. A re-encryption key can be generated for a proxy to re-encrypt from to, thus transforming (c) to another cipher text. Then, another user (u) can use own private key private to decrypt and obtain the plain piece of data.

Identity Based Encryption: Identity-Based Encryption (IBE) is a type of public key cryptography in which key pairs for a given entity are generated based on the identity of that entity. Using this kind of cryptography, a piece of data (m) can be encrypted using the identity (id) of a user (u) to obtain a cipher text (c). Then, user (u) can use his private key (priv) to decrypt (c) and obtain the plain piece of data (m). Note that no public key (pub) is used for encryption, but the identity of the user (id) is applied instead.

Identity-Based Proxy Re-Encryption: Identity-based proxy re-encryption is used for self–protection of data of the authorization model using elliptic curve cryptography. Details about the cryptographic operations that are performed by these functions can be found. A description of each function follows

- ✓ Initialize Cryptographic Schema
- ✓ Generates Secret Keys
- ✓ Generates Re-Encryption Key
- ✓ Encrypt Data
- ✓ Generate Re-Encryption Key
- ✓ Re-Encrypts Data
- ✓ Decrypts Data

Ontology Representing Authorization Model: OWL is a W3C standard which enables the specification of ontologies, defining class hierarchies and their relationships, associated properties and cardinality restrictions. This language is based on formal methods and it constitutes a remarkable added value since it provides powerful semantics to define the authorization model.

Key Management and Security Analysis: IBPRE does not use public and private key pairs in cryptographic operations. Instead, aMaster Secret Key (MSK) is used in combination with identities. This MSK is generated during the setup phase and it should be kept private. On another hand, users accessing the data need their own Secret Key (SK) to compute the decrypt () function. Secret keys are generated based on the user identity and the MSK. There are several approaches for the distribution of these keys to users. In a straightforward approach, SKs can be generated internally by the data owner to keep the MSK protected. SecRBAC provides a self-protected mechanism to upload data to the cloud assuring that no unauthorized party is able to access the data, including the CSP. In this case, the CSP is considered a curious adversary that would try to disclose the information to use it on its own benefit and b try to neglect the authorization rules in order to release the information to an unauthorized third party. The following parameters are used: the Master Secret Key, the set of parameter, identities, secret keys and re-encryption keys. Among these, the parameters and the identities id are public information, while the MSK should be kept private by the data owner or the PKG in case it is used. In turn, secret keys of authorization elements (e.g. roles, objects) should be also kept private by the data owner since they are used to generate re-encryption keys. Secret keys of users should be distributed and kept private by the corresponding users for them to be able to decrypt data. Finally, re-encryption keys are used to protect the rules in the authorization model.

5. Result Analysis:

The existing and proposed methodologies are compared with each other in terms of varying parameter values. The performance metrics that are considered for proving the improvement of the proposed methodology are

- ✓ Times changing the number of re-encryptions
- ✓ Times changing the length of encrypted data
- ✓ Times changing the length of identities

Times Changing the Number of Re-Encryptions: It is worth mentioning that the number of re-encryptions depends on the expressiveness used by the data owner when defining the authorization rules. Re-encryptions for an access request can be observed. At least one re-encryption should be done. This is the case when an access grant in the binary relation is directly granting the requesting user access to the requested object. If roles are

used, then at least two re-encryptions should be done. One for the access grant and another one for the subject role assignment in D. Then, if hierarchical expressiveness is used, several re-encryptions could be needed for the parent role and parent-object assignments in E and F, respectively. Thus, the number of re-encryptions would depend on the hierarchical levels that are defined between the role of the requesting user and the granted role plus the levels between the requested and the granted object. It should be noticed that this does not mean the number of roles or objects managed by the model, but only the levels in their hierarchies. The number of re-encryptions depends on the number of role and object levels between the subject (s1) and the object (o1). The test has been done up to 100 re-encryptions in order to stress the system, considering 100 levels in role and object hierarchies from s1 to o1. However, in practical terms a number of 10 levels (20 at most) would be enough for a realistic scenario. For this number of re-encryptions, decrypt ( ) remains under acceptable execution times.

Table 1: Times Vs Number of Re-encryptions.

Times	Number of Re-encryptions
0	10
5	20
10	30
15	40

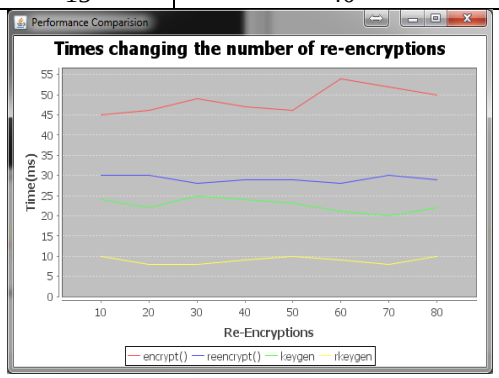

Figure 2: Times changing the number of re-encryptions

Times Changing the Length of Identities: In this approach, data is encrypted using a symmetric algorithm such as AES with a random key that is then encrypted using the asymmetric scheme. Hence, four lengths have been considered for this test: 128, 192, 256 and 512 bits. The first three correspond to the common key lengths used for AES encryption. The last one has been also added to test stronger AES encryption with 512 bytes keys. Below figure shows the results for this test. Again, results show a constant execution time for all functions. Theoretically encrypt(),re-encrypt() and decrypt() could be affected by the length of the data since they take the plain data (m) or its encrypted counterpart (c) as parameter. However, the mathematical operations within the cryptographic functions of IBPRE deal with a numeric representation that maps to numbers of the same length for all the considered lengths and performance is not affected.

Table 2: Times Vs Length of Identities

Times	Length of Identities
0	64
5	128
10	192
15	256
20	320
25	384

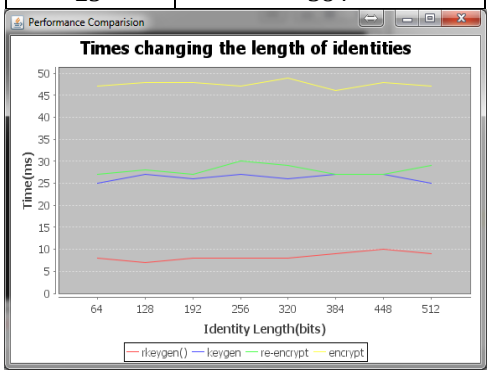

Figure 3: Times changing the length of identities

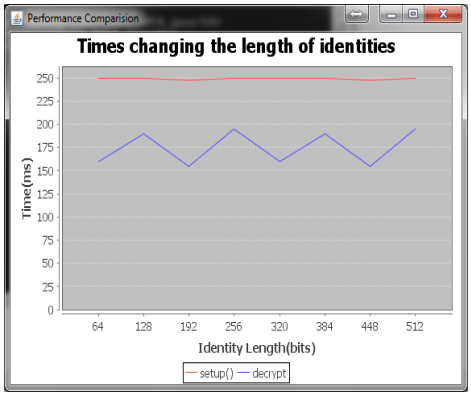

Figure 4: Times changing the length of identities

Times Changing the Length of Encrypted Data: In turn, in an IBE scheme, the length of the identities used for the cryptographic operations may also affect the execution times. Another test has been done by varying the length of the identities from 8 to 512 bytes by incrementing in 64 bytes for each execution set. below figure shows the results for this test. Results do not show any variation for the cryptographic functions. Initially, it should affect functions dealing with identities. These functions are keygen(), encrypt() and rkgen(). However, processing of these strings within the functions is so small that it is negligible for the execution time

Table 3: Time Vs Length of Encrypted Data

Time	Length of Encrypted Data
0	128
150	256
250	384

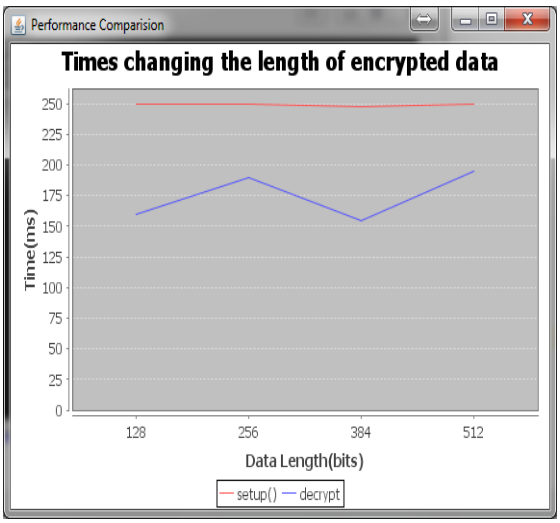

Figure 6: Times changing the length of encrypted data

References:

1. Ateniese G, Fu K, Green M, and Hohenberger S (2006), "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.
2. Bobba R, Khurana H, and Prabhakaran M (2009), "Attribute-sets: A practically motivated enhancement to attribute-based encryption", in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, Vol. 5789, pp. 587–604.
3. Coyne E and Weil T R (2013), "Abac and rbac: Scalable, flexible, and auditable access management", IT Professional, Vol. 15, no. 3, pp. 14–16.
4. Empower ID (2013), "Best practices in enterprise authorization: The RBAC/ABAC hybrid approach", White paper, pp 65.
5. Goyal V, Pandey O, Sahai A, and Waters B (2006), "Attribute-based encryption for fine-grained access control of encrypted data", in Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98.
6. Green M and Ateniese G (2007), "Identity-based proxy re-encryption", in Proceedings of the 5th International Conference on Applied Cryptography and Network Security, Heidelberg Springer-Verlag, pp. 288–306.

7. Kuhn D R, Coyne E J, and Weil T R (2010), "Adding attributes to role based access control", Computer, Vol. 43, no. 6, pp. 79–81.
8. Wang F, Liu Z, and Wang C (2015), "Full secure identity-based encryption scheme with short public key size over lattices in the standard model", International Journal of Computer Mathematics, pp. 1–10.
9. Wang G, Liu Q, and Wu J (2010), "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", in Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 735–737.
10. Waters B (2011), "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably securerealization", in Public Key Cryptography, Vol. 6571, pp. 53–70.
11. Zhang Y, Chen J, Du R, Deng L, Xiang Y, and Zhou Q (2014), "Feacs: A flexible and efficient access control scheme for cloud computing", Trust, Security and Privacy in Computing and Communications, IEEE 13th International Conference , pp. 310–319.