International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.07,Issue.05,
May-2018,
Pages:0940-0943

www.ijsetr.com

SecRBAC: Secure Data in the Clouds

MEKALA PRAVEEN KUMAR[1], M. CHANDINI[2]

[1]PG Scholar, Dept of Computer Science, Sri Govindaraja Swamy Arts College, Tirupati, AP, India.
[2]Assistant Professor, Dept of Computer Science, Sri Govindaraja Swamy Arts College, Tirupati, AP, India.

Abstract: Most current security solutions are based on perimeter security. However, Cloud computing breaks the organization perimeters. When data resides in the Cloud, they reside outside the organizational bounds. This leads users to a loos of control over their data and raises reasonable security concerns that slow down the adoption of Cloud computing. Is the Cloud service provider accessing the data? Is it legitimately applying the access control policy defined by the user? This paper presents a data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user data regardless the Cloud service provider that holds it. Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior. The authorization model provides high expressiveness with role hierarchy and resource hierarchy support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which enables advanced rule management like semantic conflict detection. A proof of concept implementation has been developed and a working prototypical deployment of the proposal has been integrated within Google services.

Keywords: Data-Centric Security, Cloud Computing, Role-Based Access Control, Authorization.

I. INTRODUCTION

Security is one of the main user concerns for the adoption of Cloud computing. Moving data to the Cloud usually implies relying on the Cloud Service Provider (CSP) for data protection. Although this is usually managed based on legal or Service Level Agreements (SLA), the CSP could potentially access the data or even provide it to third parties. Moreover, one should trust the CSP to legitimately apply the access control rules defined by the data owner for other users. The problem becomes even more complex in Inter cloud scenarios where data may flow from one CSP to another. Users may loss control on their data. Even the trust on the federated CSPs is outside the control of the data owner. This situation leads to rethink about data security approaches and to move to a data-centric approach where data are self-protected whenever they reside. Encryption is the most widely used method to protect data in the Cloud. In fact, the Cloud Security Alliance security guidance recommends data to be protected at rest, in motion and in use. Encrypting data avoids undesired accesses. However, it entails new issues related to access control management. A rule-based approach would be desirable to provide expressiveness. But this supposes a big challenge for a data-centric approach since data has no computation capabilities by itself. It is not able to enforce or compute any access control rule or policy. This raises the issue of policy decision for a self-protected data package: who should evaluate the rules upon an access request? The first choice would be to have them evaluated by the CSP, but it could potentially bypass the rules.

Another option would be to have rules evaluated by the data owner, but this implies that either data could not be shared or the owner should be online to take a decision for each access request. To overcome the aforementioned issues, several proposals try to provide data-centric solutions based on novel cryptographic mechanisms applying Attribute based Encryption (ABE). These solutions are based on Attribute-based Access Control (ABAC), 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) or ABAC is a better model for authorization. Without entering into this debate, both approaches have their own pros and cons. To the best of our knowledge, there is no data-centric approach providing an RBAC model for access control in which data is encrypted and self-protected. The proposal in this paper supposes a first solution for a data-centric RBAC approach, offering an alternative to the ABAC model. An RBAC approach would be closer to current access control methods, resulting more natural to apply for access control enforcement than ABE-based mechanisms. In terms of expressiveness, it is said that ABAC supersedes RBAC since roles can be represented as attributes. However, when it comes to data-centric approaches in which data is encrypted, ABAC solutions are constrained by the expressiveness of ABE schemes. The cryptographic operations used in ABE usually restrict the level of expressiveness for access control rules. For instance, role hierarchy and object hierarchy capabilities cannot be achieved by current ABE schemes.

Moreover, they usually lack some combination with a user-centric approach for the access control policy, where common authorization-related elements like definition of users or role assignments could be shared by different pieces of data from the same 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, 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. Role 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 self-protection, where novel criptograhpic techniques such as Proxy Re-Encryption Encryption (PRE), Identity-Based Encryption (IBE) and Identity-Based Proxy Re-Encryption (IBPRE) 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.

Each piece of data is ciphered 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 combines 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 rulebased approach for authorization in Cloud systems where rules are under control of the data owner and access control computation is delegated to the CSP, but making it unable to grant access to unauthorized parties. The main contributions of the proposed solution are:

- Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.
- Rule-based approach for authorization where rules are under control of the data owner.
- High expressiveness for authorization rules applying the RBAC scheme with role hierarchy and resource hierarchy (Hierarchical RBAC or hRBAC).
- Access control computation delegated to the CSP, but being unable to grant access to unauthorized parties.
- Secure key distribution mechanism and PKI compatibility for using standard X.509 certificates and keys.

II. RELATED WORK

Different approaches can be found in the literature to retain control over authorization in Cloud computing. 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 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 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 done when sending a file or document to a specific receiver and ensures that only the receiver with the appropriate key is able to decrypt it. From an authorization point of view, this can be seen as a simple rule where only the user with privilege to access the data will be able to decrypt it (i.e. the one owning the 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 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.

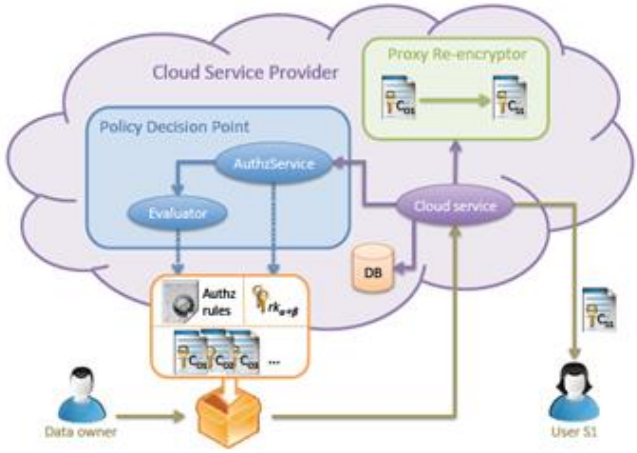

Fig.1. Architecture for deployment in a CSP.

III. PROXY RE-ENCRYPTION AND IDENTITY-BASED ENCRYPTION

SecRBAC makes use of cryptography to protect data when moved to the Cloud. Advanced cryptographic techniques are used to protect the authorization model in order to avoid the CSP being able to disclose data without data owner consent. Concretely, the solution is based on Proxy Re-Encryption (PRE). 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 α and β, the proxy could re-encrypt a ciphertext c_α encrypted under α public key to another ciphertext c_β that can be decrypted using β private key. Using this kind of cryptography, a user u_α can encrypt a piece of data m using his own public key pub_α to obtain a ciphertext c_α. A re-encryption key $rk_{\alpha\to\beta}$ can be generated for a proxy to re-encrypt from α to β, thus transforming c_α to another ciphertext c_β. Then, another user u_β can use his own private key $priv_\beta$ to decrypt c_β and obtain the plain piece of data m. Several works in this direction have arisen, resulting in diverse Proxy Re-Encryption schemes with different features. The solution proposed in this paper is not tied to a concrete PRE scheme or implementation. However, not all the available PRE schemes are suitable to achieve the goals of this research. In order to characterize and compare different schemes, provided a set of features relevant to proxy re-encryption. Based on this characterization, the following set of features are required by the Proxy Re-Encryption scheme used for the proposal in this paper:

- **Unidirectionality:** A unidirectional scheme enables the generation of a re-encryption key $rk_{\alpha\to\beta}$ without allowing re-encryption from β to α.
- **Non-interactivity:** A non-interactive scheme enablesa user u_α to construct a re-encryption key $rk_{\alpha\to\beta}$without the participation of u_β or any other entity.
- **Multi-use:** A multi-use scheme enables the proxy to perform multiple re-encryption operations on a single ciphertext. That is, to re-encrypt from c_α to c_β, from c_α to c_γ and so on.

The following set of functions is provided by IBPRE. It constitutes the cryptographic primitives for the proposal:

$$\text{setup}(p, k) \to (p, msk) \quad (1)$$

$$\text{keygen}(p, msk, id_\alpha) \to sk_\alpha \quad (2)$$

$$\text{encrypt}(p, id_\alpha, m) \to c_\alpha \quad (3)$$

$$\text{rkgen}(p, sk_\alpha, id_\alpha, id_\beta) \to rk_{\alpha\to\beta} \quad (4)$$

$$\text{reencrypt}(p, rk_{\alpha\to\beta}, c_\alpha) \to c_\beta \quad (5)$$

$$\text{decrypt}(p, sk_\alpha, c_\alpha) \to m \quad (6)$$

A brief description of each function follows.

- **Initializes the Cryptographic Scheme:** It takes as input a security parameter k to initialize the cryptographic scheme (e.g. parameters to generate an elliptic curve) and outputs both the Master Secret Key msk and a set of public parameters p that is used as input for the rest of functions.
- **Generates Secret Keys:** It takes as input the msk and an identity id_α, and outputs the Secret Key sk_α corresponding to that identity.
- **Encrypts data:** It takes as input an identity id_α and a plain text m, and outputs the encryption of m under the specified identity c_α.
- **Generates Re-Encryption Keys:** It takes as input the source and target identities id_α and $id_{\alpha\to\beta}$ as well as the Secret Key of the source identity sk_α, and outputs the Re-encryption Key $rk_{\alpha\to\beta}$ that enables to re-encrypt from id_α to id_β.
- **Re-Encrypts Data:** It takes as input a ciphertext c_α under identity id_α and a Re-encryption Key $rk_{\alpha\to\beta}$, and outputs the re-encrypted ciphertext c_β under identity id_β.
- **Decrypts Data:** It takes as input a ciphertext c_α and its corresponding Secret Key sk_α, and outputs the plain text m resulting of decrypting c_α.

IV. AUTHORIZATION MODEL WITH ENRICHED ROLEBASED EXPRESSIVENESS

The management of access control and security could become a difficult and error prone task in distributed systems like Cloud computing. Authorization models providing high expressiveness can help to control and manage security and to deal with this complexity. 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. Role-Based Access Control (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. To illustrate the concepts described along this paper, let us consider an example where a company uploads to the Cloud a couple of documents called DocumentX and DocumentY which could be accessed only by the managers of the company. Also consider that Bob and Alice are managers of this company. Without role support in the authorization model, the company should define and manage individual privilege assignments for every user and every document.

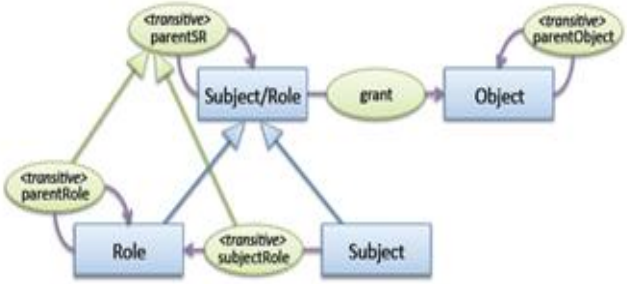

Fig.1. Ontology representing the authorization model.

That is, four privileges should be defined in this example: Bob → DocumentX, Bob → DocumentY , Alice → Document X and Alice → DocumentY . On the other hand, making use of roles, a Managers role could be defined to group all users that are managers of the company and two single privileges need to be defined: Managers → Document X and Managers → DocumentY . Let us denote them p_1 and p_2, respectively. This provides more expressiveness to the model, making it more natural for the administrator to manage privileges, as well as avoiding the need to manage individual privileges.

V. CONCLUSION

A data-centric authorization solution has been proposed for the secure protection of data in the Cloud. SecRBAC allows managing authorization following a rule-based approach and provides enriched role-based expressiveness including role and object hierarchies. Access control computations are delegated to the CSP, being this not only unable to access the data, but also unable to release it to unauthorized parties. Advanced cryptographic techniques have been applied to protect the authorization model. A re-encryption key complement each authorization rule as cryptographic token to protect data against CSP misbehavior. The solution is independent of any PRE scheme or implementation as far as three specific features are supported. A concrete IBPRE scheme has been used in this paper in order to provide a comprehensive and feasible solution. A proposal based on Semantic Web technologies has been exposed for the representation and evaluation of the authorization model. It makes use of the semantic features of ontologies and the computational capabilities of reasoners to specify and evaluate the model. This also enables the application of advanced techniques such as conflict detection and resolution methods. Guidelines for deployment in a Cloud Service Provider have been also given, including an hybrid approach compatible with Public Key Cryptography that enables the usage of standard PKI for key management and distribution. A prototypical implementation of the proposal has been also developed and exposed in this paper, together with some experimental results. Future lines of research include the analysis of novel cryptographic techniques that could enable the secure modification and deletion of data in the Cloud. This would allow to extend the privileges of the authorization model with more actions like modify and delete. Another interesting point is the obfuscation of the authorization model for privacy reasons. Although the usage of pseudonyms is proposed, but more advanced obfuscation techniques can be researched to achieve a higher level of privacy.

VI. 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] InterNational 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 rolebased 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.

Author's Profile:

Mekala Praveen Kumar, I was Received Graduate Degree In B.Sc Computer Science, From A.S. Degree College, Tuggali in the year of 2013-2016. Pursuing post Graduate Degree, M.Sc Computer Science from Sri Govindaraja Swamy Arts College, Affiliated to Sri Venkateswara University, Tirupati in the year of 2016-2018.

Ms. M Chandini is Received her B.Tech (CSE) From JNTUA and MBA Received her Post Graduate from Sri Venkateswara University.