PROVIDING SECURITY TO DATA STORED ON CLOUDS USING ROLE BASED APPROACH FOR DATA CENTRIC APPROACH.

Shila D. Ravte[1], Prof. Priti Subramanium [2]

[1]*M.E. Student, Dept. of Computer Science and Engineering, SSGBCOET, Bhusawal, Maharashtra, India*
[2]*Assistant Professor, Computer Science and Engineering, SSGBCOET, Bhusawal, Maharashtra, India*

ABSTRACT

Most present security arrangements are based on perimeter security. However, Cloud computing breaks the organization borders. When data stored on the Cloud, So indirectly data reside outside the organizational boundaries. This may leads users to lost control over their data and raises security issues that slow down the use of Cloud computing. Data-centric access control approach with role-based expressiveness in which security is concern on protecting user data regardless the Cloud service provider who is responsible to hold data. Identity-based and proxy re-encryption techniques are used to Securing the authorization model. Data is encrypted and authorization rules are cryptographically protected to stored user data against the service provider access or misbehavior. The authorization model provides very high expressiveness with role hierarchies and resource hierarchical support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which make possible 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.

Keyword: *Data-Centric Security, Role-Base Access Control, Cloud Computing***.**

1. INTRODUCTION

Security is one of the main issue user consider while using Cloud Computing. Moving data to cloud usually user is dependent on Cloud service provider (CSP) for data protection. Whereas this management is based on legal or Service Level Agreements (SLA), in this situation CSP may potentially access the data or he can provide it to third parties. So user should trust the CSP to apply the access control protocol specified by the data owner for different users. The main problem arises in Inter-cloud scenarios where data exchange from one CSP to another CSP. Sometimes users may loss control on their data. Even the trust on the united CSPs is out of the control of the data owner. This situation leads to think about data security approaches again and to move to a data-centric approach so that we can ensure that data are self-protected whenever they reside. Encryption is the most commonly used method to provide security to data in the Cloud. Encrypting data avoids unauthorized accesses. However, it requires new issues related to access control management. A rule-based strategy would be suitable to provide expressiveness. But this big challenge for a data-centric approach as data has no computation capabilities by itself. It is not able to determine or compute any access control rule policy. This raises the problem of policy decision for a self-protected data package: who should examine the rules upon an access request? The first choice would be to have them calculated by the CSP, but it may bypass the rules. Another option would be to have rules determined by the data

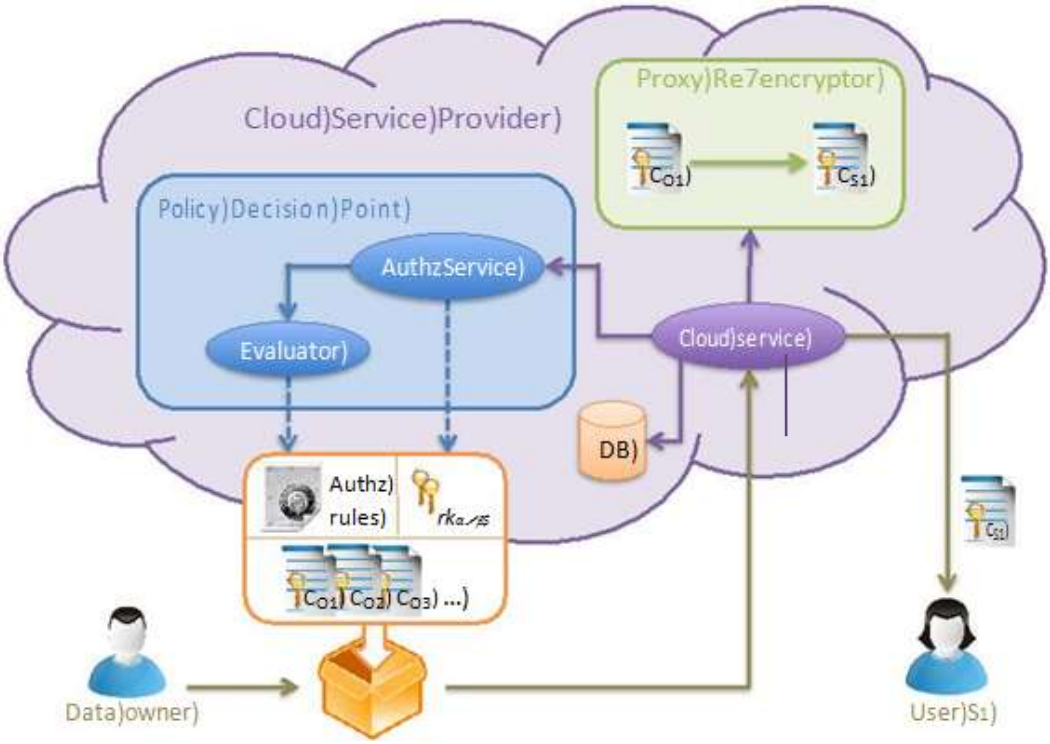
owner, but this entail that either data could not be shared or the owner should be online to make a decision for each access request. To overcome this issues, several proposals try to provide data-centric solutions based on Attribute-based Encryption (ABE). This is based on Attribute-based Access Control (ABAC), in which accesses are granted to users according to set of attributes. But there is no data-centric approach providing an RBAC approach for access control in which data is encrypted and self-protected. The proposal in this paper considers a first solution for a data-centric RBAC model, offering an alternative solution to the ABAC model. An RBAC approach would be closer to current access control strategies, resulting more natural to apply for access control effectiveness than ABE-based mechanisms. This paper presents a data-centric access control strategy for self-protected data that can run in mistrusted CSPs and provides extended Role-Based Access Control. The proposed authorization solution provides a rule-based model by using the RBAC scheme, where roles are used to simplify the management of access to the resources. This approach can help to control and manage

2. LITERATURE SURVAY

Different strategies can be found in the literature to gain control over authorization in Cloud computing. In [13] authors propose to keep the authorization decisions taken by the data owner only. The access model is not explore to the Cloud but kept secure on the data owner premises. However, in this strategy the CSP becomes a mere storage system and the data owner should be online to response access requests from users. Another approach from [14] deals with this issue by enabling a plug approach in the CSP that allows data owners to prepare their own security modules. This permits to control the authorization model used within a CSP. However, it does not establish how the authorization model should be secured, so the CSP could infer information and access the data. Moreover, this strategy does not cover Inter-cloud scenarios, since the plug-in module should be delivered to different CSPs. Additionally, these strategies do not protect data with encryption methods. In the proposed data encryption is used to prevent the CSP to access the data or to release it bypassing the authorization strategies. However, applying data encryption entails additional challenges related to authorization expressiveness. Following a direct approach, one can include data in a package encrypted for the authorized users. This is done while sending a file or document to a specific receiver and assures 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 authorized user to access the data will be able to decrypt it (i.e. the one owning the key). However, no access control expressiveness is delivered by this approach. Only that simple rule can be emphasized and just one single rule can apply to each data package. Thus, multiple encrypted copies should be created in order to deploy the same data to different receivers. To cope with these issues, a data-centric approach that is able to cryptographically secure the data while providing access control capabilities. Several data-centric approaches, mostly based on Attribute-based Encryption (ABE) [5], have developed for data protection in the Cloud [4]. In ABE, encrypted cipher-text is labeled with a set of attributes defined by the data owner. Users also have a set of attributes with their private keys. They would be able to access data (i.e. decrypt it) or not depending on the match between cipher-text and key attributes. User required attribute to decrypt the data specified by an access structure, which is defined as a tree with AND , OR nodes. There are two main strategies for ABE depending on where the access structure resides: Key-Policy ABE (KP-ABE) [5] and Cipher-text-Policy ABE (CP-ABE) [3]. In KP-ABE the access structure or policy is defined within the private keys of users. This allows encrypting data with attributes as labeled and then controlling the access to such data by delivering the appropriate keys to users. However, in this case the policy is defined by the key issuer not by encryptor of data, i.e. the data owner. So, the data owner should trust the key issuer for this to properly generate an appropriate access policy. To solve this issue, CP-ABE suggests to include the access structure within the cipher-text, which is under control of the data owner. Then, the key issuer just affirm the attributes of users by including them in private keys.. Different proposals have been also developed to try to alleviate ABE expressiveness prescription. Authors in [15] propose a solution based on CP-ABE allows sets of attributes called Cipher-text Policy Attribute Set Based Encryption (CP-ASBE). Attributes are arranged in a recursive set structure and access policies can be defined upon a single set or joining attributes from multiple sets. The definition of compound attributes and specification of policies that influence set of attributes. An strategy named Hierarchical Attribute-based Encryption is presented in [16]. It uses a hierarchical generation of keys to achieve subtle access control, scalability and

delegation. However, this strategy implies that attributes should be managed by the same root domain authority. In [16], authors extend CP-ASBE with a hierarchical structure to users in order to improve scalability and flexibility. This approach provides a hierarchical solution for users within a domain, which is obtained by a hierarchical key structure. One more approach is Flexible and Efficient Access Control Scheme (FEACS) [2]. It is based on KP-ABE and provides an access control structure represented by a formula which include AND, OR and NOT, enabling more expressiveness for KP-ABE. Above mentioned ABE-based solutions proposed for solving access control in Cloud computing are based on the Attribute-based Access Control (ABAC) model. ABAC and RBAC both models have their own advantages and disadvantages [7] [9]. On one hand, RBAC may require the specification of a large number of roles for detailed authorization (role explosion problem in RBAC). ABAC is also easier to set up without need to make an effort on role description as needed for RBAC. On another hand, ABAC may result in a huge number of rules since a system with n attributes would have up to 2^n possible rule combinations (rule explosion problem in ABAC). ABAC differentiate authorization rules from user attributes, making it difficult to determine permissions available to a particular user, while RBAC is deterministic and user privileges can be easily obtained by the data owner. Moreover, the cryptographic operations used in ABE approaches usually repress the level of expressiveness provided by the access control rules. Concretely, role hierarchy and object hierarchy capabilities provided by Secure RBAC can-not be obtained by current ABE schemes. Moreover, a private key in ABE requires the attributes of the user, which tights the keys to permissions in the access control policy. In Secure RBAC, user keys only recognize their holders and they are not tied to the authorization model. That is, user access right are completely independent of their private key. Finally, no user-centric approach for authorization rules is proposed by current ABE solutions. In Secure RBAC, a single access policy specified by the data owner is able to secure more than one piece of data, resulting in a user-centric approach for rule management.

3. SYSTEM ARCHITECTURE



Above figure shows Working of proposed system in which the application of these functions make use of the re-encryption scheme to lose the Multi-use feature, which is needed as described in this paper. That is, once a Re-encryption Key generated is used to re-encrypt, no further re-encryptions allowed to that encrypted object. However, for the purposes of authentication in this paper, this kind of re-encryption only required to be

done to re-encrypt the protected object And this is executed in the last re-encryption, which is the one that results in the data being encrypted using the user public key. Thus, re-encryption keys generated with the original function should still be applied for re-encryptions along the authorization path, without the one affecting the user, which is the last re-encryption. With this strategy, the data owner uses the public key while defining rules in the authorization model. When user send a request, the data object is re-encrypted by using user public key. So that user can then decrypt the data by using the appropriate private key.

When data is moved to the cloud, Data owner generate a self-protected package This package includes: the encrypted data objects, the authorization rules and the corresponding re-encryption keys. Data objects are encrypted at the time of uploading them to the Cloud in order to prevent the CSP to access them. This step is performed by data owners by using the encrypt() function. Data must be encrypted using the identity of the object which is going to uploaded . A digital envelope approach can be used to protect data objects without applying direct encryption. This would extends crypto-graphic operations like re-encryptions for large number of data objects. This strategy consists in using a symmetric encryption algorithm (e.g. AES) to protect the data object at its own. The encryption of data is done by using a random symmetric key generated for the single encryption. Then, this key is encrypted using the encrypt() function. By using this procedure, big objects (e.g. large documents) are encrypted using symmetric cryptography, by using more efficient algorithms. Authorization rules are specified by the data owner and directly mapped into the authorization model. This is done by considering the corresponding elements in the binary relations.

Advantages

There are many advantages of proposed system listed below:

1. The proposal in this paper consider a first solution for a data-centric RBAC approach, offers an alternative to the ABAC model.

2. Proposed scenario can help to control and manage security and to handle the complexity of managing access control in Cloud computing.

3. Resource and role hierarchies are acceptable by the authorization model, which provide more expressiveness to the rules by enabling the definition of simple but powerful rules that apply to several resource and users thanks to privilege propagation through hierarchies and roles.

4. Policy rule specifications are relay on Semantic Web technologies that enable enriched rule definitions and advanced policy management features like conflict detection.

4. CONCLUSIONS

A data-centric authorization solution has been introduced to provide security to data stored on Cloud. Secure RBAC allow to manage authorization which follow rule-based approach and provides high -leveled role-based expressiveness including object and role hierarchies. Access control computations are delegated to the CSP, being this not only unable to data the access, but also not able to release it to unauthorized parties. Advanced cryptographic strategies have been applied to provide security to the authorization model. A re-encryption key complement each authorization rule as cryptographic token to provide security to data against CSP misbehavior. A concrete IBPRE technique has been used in order to provide a comprehensive and feasible option with Public Key Cryptography that enables the usage of standard PKI for key distribution and management. Future lines of research include the detailed study of novel cryptographic techniques that could enable the modification and deletion of data on the Cloud. This would allow to expand the privileges of the authorization model with more actions like delete and modify. One more interesting point is the obscure of the authorization model for privacy reasons. Although the

usage of pseudonyms is introduces, but more advanced obfuscation techniques can be researched to achieve a higher level of security.

5. 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, "Cipher text-policy attribute-based encryption: An ex-pressive, 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 Communi-cations 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 Cryptog-raphy 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 Interna-tional Conferesnce 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.

[15] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[16] G. Wang, Q. Liu, and J. Wu, "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, ser. CCS '10, New York, NY, USA, 2010, pp. 735–737.