ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Protection using RBAC and CPABE in Cloud Computing Infrastructure

U. Prema
Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana - 500014, India.

D. Kalpana
Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana - 500014, India.

Abstract:
Data Protection using RBAC and CPABE in Cloud Computing Infrastructure is a project which develops a self-contained data protection mechanism called RBAC-CPABE by integrating role-based access control (RBAC), which is widely employed in enterprise systems, with the cipher text-policy attribute-based encryption (CP-ABE). This project presents a data-centric RBAC (DC-RBAC) model that supports the specification of fine-grained access policy for each data object to enhance RBAC's access control capabilities. A security analysis and experimental results indicate that RBAC-CPABE maintains the security and efficiency properties of the CP-ABE scheme on which it is based, but substantially improves the access control capability. This project presents an implemented framework for RBAC-CPABE to protect privacy and enforce access control for data stored in the cloud.

1. INTRODUCTION:

In cloud computing, an increasing number of enterprises and organizations use cloud servers as their system platform. Today, role-based access control (RBAC) model is the most popular model used in enterprise systems; however, this model has severe security problems when applied to cloud systems. A classic RBAC model uses reference monitors running on data servers to implement authorization. However, the servers in the cloud are out of the control of enterprise domains and, therefore, must be considered untrusted by default. Hence, building an effective data protection mechanism for cloud-based enterprise systems has become a major challenge.

Currently, encryption is the primary mechanism used in clouds to ensure data security. The Cloud Security Alliance (CSA) [1] suggests that an excellent method of increasing data security is to keep data encrypted both in transit and when stored within the cloud. Although classic encryption schemes such as public-key encryption and identity based encryption (IBE) [2] can ensure data confidentiality, they cannot enforce effective access control. However, if the encrypted data were to feature an internalized access policy and was able to authorize or deny users based on the access policy, then confidentiality and access control could be achieved by the data itself rather than having to rely on the untrusted cloud servers.

This type of protection model, which is referred to as self-contained data protection n this paper not only minimizes the reliance on the cloud servers but also prevents unauthorized data access and tampering during transmission. self-contained data protection essentially gives data the ability to ensure its own security, and it is an effective mechanism to protect data in cloud. However, neither RBAC alone or classic public encryption—or even the combination of both techniques [3]–[5] can satisfy the requirements of self-contained data protection. The reasons are as follows:

- In RBAC, access permissions are assigned through roles and cannot be directly assigned to a user, which is insufficiently fine-grained.

Cite this article as: U. Prema & D. Kalpana, "Data Protection using RBAC and CPABE in Cloud Computing Infrastructure", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5, Issue 6, 2018, Page 295-300.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For example, suppose that user ux needs to be granted permission p. In the RBAC model there are two ways to achieve this goal. The first approach is to assign the permission p to one of ux's rolesr. However, it means that all users who are assigned to role r are also granted permission p, which may introduce security problems. The second approach is to add a new role r' and assign it to ux. Although this approach solves the problem raised by the first approach, adding an additional role r' increases the complexity of the system—especially when such authorizations are very frequent. Thus, neither approach can effectively achieve the goal.

- RBAC describes an access control policy for the full collection of data in the entire enterprise rather than for each data object. By defining roles and assigning those roles to users, RBAC can achieve data protection. However, data is only one constituent of a system (i.e. users, roles, permission assignments and so forth can have constraints, but data cannot). Hence, RBAC is targeted mainly to integral control of the data in the system, but it cannot meet the specific security requirements of each data object.
- RBAC needs to be implemented using reference monitors that run on the data servers. Because cloud servers may not always be trusted, depending on them to enforce access control introduces insecurities into the system.

Therefore, the RBAC model and its enforcement mechanism cannot be directly applied to a self-contained data protection mechanism. Attribute-based encryption (ABE) [7] provides support for self-contained data protection. In ABE, both a user's private key and the ciphertext are associated with some attributes. When the attributes used in the ciphertext and the attributes in a user's private key match, the user can decrypt successfully. In this way, ABE achieves both encryption and access control simultaneously.

There are two variants of ABE, namely, key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the ciphertext is associated with a set of attributes and the private key is associated with an access policy. In CP-ABE, the concept is reversed: the ciphertext is associated with an access policy and the private key is associated with a set of attributes. Between these two variants of ABE, CP-ABE is more suitable for an enterprise environment, and it is an ideal fundamental scheme for implementing a self-contained data protection mechanism. In this paper, we construct a self-contained protection mechanism for outsourced enterprise data. In addition to being compatible with the existing RBAC system, our method also allows users to specify other required policies for each data object. Compared with traditional protection mechanisms, the most prominent characteristic of our solution is that it gives data the ability to ensure its own security using both encryption and a classic access control model without depending on the servers on which it resides. The contributions of this paper are presented as follows.

- To specify a flexible access policy for each data object under RBAC model, we propose a data-centric RBAC (DC-RBAC) model. In DC-RBAC, the access policy is bounded by data, which supports self-contained data protection. In addition to role constraints, DC-RBAC also contains user attribute constraints and environment constraints, which correspond to information about the authorized users and contextual information about the environment, respectively. Hence, DC-RBAC is a more expressive and fine-grained access control model.

We integrate DC-RBAC with a CP-ABE scheme (i.e. ECP-ABE) and propose a self-contained data protection scheme called RBAC-CPABE. To support all types of constraints with DC-RBAC, we first extend ECP-ABE to support role assignment and inheritance.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Then, we present a mapping model to transform the DC-RBAC access policy to the ECP-ABE access tree. Finally, the data object is encrypted with ECP-ABE. Through this design, RBAC-CPABE gives data the ability to carry fine-grained access policy and enforce access control entirely by itself.

2. LITERATURE SURVEY

2.1 Cryptographic role-based security mechanisms based on role-key hierarchy

In this paper, we propose a practical cryptographic RBAC [8] model, called role-key hierarchy model, to support various security features including signature, identification and encryption based on role-key hierarchy. With the help of rich algebraic structure of elliptic curve, we introduce a role-based cryptosystem construction to verify the rationality and validity of our proposed model. Also, a proof of-concept prototype implementation and performance evaluation is discussed to demonstrate the feasibility and efficiency of our mechanisms.

2.2 Provably secure role-based encryption with revocation mechanism

In this paper, we present a practical RBE scheme with revocation mechanism based on partial-order key hierarchy with respect to the public key infrastructure, in which each user is assigned with a unique private-key to support user identification, and each role corresponds to a public group-key that is used to encrypt data. Based on this key hierarchy structure, our RBE scheme allows a sender to directly specify a role for encrypting data, which can be decrypted by all senior roles, as well as to revoke any subgroup of users and roles. We give a full proof of security of our scheme against hierarchical collusion attacks. In contrast to the existing solutions for encrypted file systems, our scheme not only supports dynamic joining and revoking users, but also has shorter cipher texts and constant-size decryption keys.

3. OVERVIEW OF THE SYSTEM

3.1 EXISTING SYSTEM

In the existing system, encryption is the primary mechanism used in clouds to ensure data security. The Cloud Security Alliance (CSA) suggests that an excellent method of increasing data security is to keep data encrypted both in transit and when stored within the cloud. Although classic encryption schemes such as public-key encryption and identity based encryption (IBE) [2] can ensure data confidentiality, they cannot enforce effective access control. However, if the encrypted data were to feature an internalized access policy and was able to authorize or deny users based on the access policy, then confidentiality and access control could be achieved by the data itself rather than having to rely on the un-trusted cloud servers.

3.2 PROPOSED SYSTEM

The proposed system not only minimizes the reliance on the cloud servers but also prevents unauthorized data access and tampering during transmission. Therefore, self-contained data protection essentially gives data the ability to ensure its own security, and it is an effective mechanism to protect data in cloud. However, neither RBAC alone or classic public encryption or even the combination of both techniques can satisfy the requirements of self-contained data protection. To address the data protection problem in cloud computing, we propose and implement a role-based self-contained data protection scheme called RBAC-CPABE.

ARCHITECHTURE

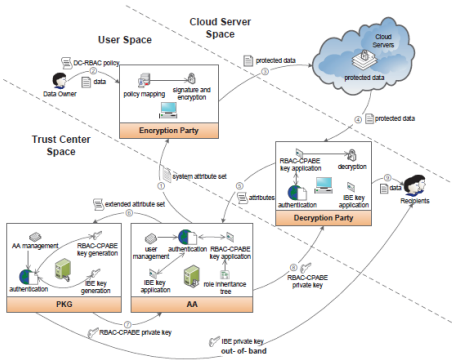

Fig 3.1 Architecture Diagram

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4. MODULES

Owner:

Data owners define access policies and encrypt data in the Encryption Party. To publish data to a cloud server, the data owner uses the data and the DC-RBAC access policy as input. Then, the access policy is mapped to the equivalent extended tree with the policy mapping module. Next, the data is signed with the user's IBE private key and hybrid encryption is enforced using the signature and encryption module. More specifically, the data is encrypted with AES while the private key of AES is encrypted by RBAC-CPABE using the access policy tree. Finally, the cipher text, consisting of the AES cipher text, the RBAC-CPABE cipher text, the access tree and the signature, is published to the cloud server.

User:

Data access is achieved through the Decryption Party. The data access process consists of two Integral steps as described in Section 5.3.2 (i.e. private key application and data decryption). Using the RBAC-CPABE private key application module, the leaf nodes and extended leaf nodes of the access tree attached in the cipher text are extracted and sent to AA along with the user's identity, forming a request to apply for an RBAC-CPABE private key. Before sending, the message is signed with the user's IBE private key. Users without an IBE private key must first apply for one through the IBE private key application module .After receiving the message from AA, the Decryption Party verifies the signature with the authentication module and then extracts the RBAC-CPABE [8] private key. If the user's attributes satisfy the access policy, the decryption module will be able to decrypt the RBAC-CPABE cipher text to obtain the AES private key with which the original data can be decrypted.

AA:

The AA is responsible for authenticating users' attributes and invoking PKG to generate private keys. When receiving a message from a user, AA first verifies whether the message is from a valid user using the authentication module. If it is a valid message, AA analyzes the request type, which can be either an IBE private key request or a RBAC CPABE private key request. If the request is for an IBE private key, AA extracts the identity of the user and sends it to PKG through the IBE private key application module. If the request is for a RBAC-CPABE [10], [11] private key, AA extracts the user's information through the management module with the user's identity. Then the RBAC-CPABE private key application module is used to verify the extended attributes with the user information and the role inheritance tree and generate the extended attribute set, which is sent to PKG to yield the user private key.

PKG:

The main function of PKG in our framework is to generate private keys. Similar to AA, after receiving a message, PKG first verifies whether the message is from a valid AA using the authentication module and AA management module. When the request is valid, PKG [7] generates the private key using either the IBE [2] private key generation module or the RBAC-CPABE private key generation module according to the request type. The IBE private key is distributed physically, while the RBAC-CPABE private key is returned to the AA after being signed.

Then AA signs and returns the message to the user after verifying the validity of PKG. As the above process shows, by adopting RBAC-CPABE, data gains the ability to determine whether to authorize users depending entirely on an access policy embedded within the data itself. Therefore, this implementation of RBAC-CPABE can eliminate the dependence on third-party servers and can achieve self-contained data protection.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5. Output Screens

Fig 8.1: Lead Registration Page

Fig 8.2: File Upload Page

Fig 8.3: Assigning Private Key Page

Fig 8.4: User Registration Page

Fig 8.5: Download Page

6. CONCLUSION

Based on the classic RBAC model, we first propose a data-centric access control model, DC-RBAC, which allows the data owner to specify individualized RBAC policies for each data object. Besides role-level constraints, DC-RBAC also contains user attribute constraints and environment constraints, which correspond to information about the authorized users and contextual information about the environment, respectively. Hence, DC-RBAC achieves more flexible and fine-grained access control.

7. REFERENCES

[1] C. S. Alliance. (2011) Security guidance for critical areas of focus in cloud computing v3.0. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology–CRYPTO . California, USA: Springer Berlin Heidelberg, 19-23 August 2001, pp. 213–229.

[3] Y. Zhu, G.-J. Ahn, H. Hu, and H. Wang, "Cryptographic role-based security mechanisms based on role-key hierarchy," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China: ACM, 13-16 April 2010, pp. 314–319.

[4] Y. Zhu, H.-X. Hu, G.-J. Ahn, H.-X. Wang, and S.-B. Wang, "Provably secure role-based encryption with

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

revocation mechanism," Journal of Computer Science and Technology , vol. 26, no. 4, pp. 697–710, 2011.

[5] Y. Zhu, G. J. Ahn, H. Hu, D. Ma, and S. Wang, "Role-based cryptosystem: A new cryptographic rbac system based on role-key hierarchy," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2138–2153, 2013.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005, vol. 3494. Aarhus, Denmark: Springer Berlin Heidelberg, 22-26 May 2005, pp. 457–473.

[7] 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. Alexandria, Virginia, USA: ACM, 30 October-3 November 2006, pp. 89–98.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy . Berkeley, CA: IEEE, 20-23 May 2007, pp. 321–334.

[9] Y. Zhu, D. Huang, C. J. Hu, and X. Wang, "From rbac to abac: Constructing flexible data access control for cloud storage services," IEEE Transactions on Services Computing, vol. 8, no. 4, pp. 601–616, July 2015.

[10] B. Lang, R. Xu, and Y. Duan, "Extending the ciphertext-policy attribute based encryption scheme for supporting flexible access control," in Proceedings of the 10th International Conference on Security and Cryptography. Reykjavik, Iceland: IEEE, 29-31 July 2013, pp. 1–11.

[11] D. Ferraiolo and R. Kuhn, "Role-based access control," in 15th National Computer Security Conference . Baltimore, Maryland: National Institute of Standards and Technology, 13-16 October 1992,p. 554 lC563.

Author's Details:

U. Prema
Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana - 500014, India.

D. Kalpana
Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana - 500014, India.