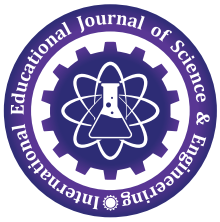
Computer Science

E-ISSN No : 2581-6195 | Volume : 2 | Issue : 2 | Mar-Apr 2019



TRUST ENHANCEMENT USING RING SIGNATURE FOR RBAC IN CLOUD STORAGE

SNEHA K S

ABSTRACT

Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. To protect the privacy of data stored in the cloud cryptographic role -based access control (RBAC) schemes have been developed to ensure that data can only be accessed by those who are allowed by access policies. Trust models improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. The existing trust models to assist (i) the data owners to evaluate the trust on the roles in a RBAC system and use this trust evaluation to decide whether to store their encrypted data in the cloud for a particular role, and (ii) the roles to evaluate the trust on the users in the RBAC system and use this trust in the decision to grant the membership to a user.The proposed system ensures a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes along with ring signature. Ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group member's keys was used to produce the signature. A ring signature scheme is a triple of ppt algorithms (Gen, Sign, and Vrfy) that, respectively, generate keys for a user, sign a message, and verify the signature of a message.

KEYWORDS: RBAC, Tust Models, Ring Signature, RBE

1. INTRODUCTION

Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the Internet or "cloud". It is maintained, operated and managed by a cloud storage service provider on a storage server that is built on virtualization techniques .Now a days, cloud storage is becoming overwhelming popular and considered as an inevitable technology in the IT world. It refers to a network of computers owned by one person or company, where other people or companies can store their data. There has been a rapid growing trend in the recent times in using online services. A major benefit of using online services is that users can store their data online and access it from anywhere. However, many online service providers do not have the capacity to store large amount of user's data due to high maintenance cost and complexity. Cloud services such as cloud storage services are providing solutions to address these issues with the ability to store and manage increasing amount of user's data stored online. Online service providers can outsource user's data to the public cloud while focusing on the service quality. Since a public cloud is an open platform, and can be subjected to malicious attacks from both insiders and outsiders, this has raised several security issues such as how to control and prevent unauthorised access to data stored in the cloud; this also applies to cloud providers themselves as the owners of the data may not wish the cloud providers to view or access its content.

At the simplest level, cloud storage can just be one user with access to one server. A user would upload his data through a terminal and store it on a server for safe keeping. In that scenario, when the server is down, retrieving your data files would be impossible task until that server came back online. From a customer's point of view, this system would be highly ineffective as it would be unreliable and consumers would reject such systems. For the idea of cloud storage to be a feasible business, the simplest level of cloud storage would have to be expanded immensely to address the issue of reliability.

One approach to protect the privacy of the data stored in the cloud is using access controls. Many access control models have been proposed over the years in the literature. In this context, role-based access control (RBAC) is a well-known access control model which can help to simplify security management especially in large-scale systems. In RBAC, roles are used to associate

Master Of Engineering, Dept. of CSE, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, India.

HOW TO CITE THIS ARTICLE:
SNEHA K S (2019). Trust Enhancement Using Ring Signature for Rbac in Cloud Storage, International Educational Journal of Science and Engineering (IEJSE), Vol: 2, Issue: 2, 01-04

Research Paper

users with permissions on resources.

In traditional systems, access control policies are usually specified and enforced by a central authority who has administrative control over all the resources in the system. However in a distributed system such as a cloud, there may not exist. such a central authority as the data may be stored in distributed data centres which cannot be under the control of a single authority. In some cases though the access control policies may be specified by the cloud provider authority itself in a centralised way, there could be multiple authorities to enforce these access policies distributed throughout the cloud system. Therefore there would be a need to trust these authorities to specify correctly the access control policies and enforce them properly.

In a cloud data storage system, the data owners would wish to specify the policies as to who can access their data and the cloud providers are required to correctly enforce the policies that the data owners have specified. In order to enforce the specified access control policies before putting the data onto the cloud, the data owners can encrypt the data in the way that only users that the owners wished to allow as specified in the access control policies are able to decrypt and access the data. Several cryptographic schemes have been developed to enforce access policies on outsourced data. These schemes combine cryptographic techniques and access control to protect the privacy of the data in an outsourced environment.

2. EXISTING SYSTEM

The main contributions of this existing system are trust models for securing data storage in cloud storage systems that are using cryptographic RBAC schemes. Though there exists many works on trust models in RBAC, none of these works consider the trust for users on the RBAC system itself. The existing trust models address the missing aspect of trust in cryptographic RBAC schemes to secure data storage in the cloud, and can provide better protection of stored data than using cryptographic approaches alone. Thus came trust models to assist (i) the data owners to evaluate the trust on the roles in a RBAC system and use this trust evaluation to decide whether to store their encrypted data in the cloud for a particular role, and (ii) the roles to evaluate the trust on the users in the RBAC system and use this trust in the decision to grant the membership to a user. It refers to these trust models as Owner-Role RBAC and Role-User RBAC trust models respectively.

Trust Issues In Using Cryptographic Rbac Schemes In Secure Cloud Storage

By using cryptographic RBAC schemes in cloud storage systems, a data owner can encrypt the data to a role, and only the users who have been granted the membership to the role or the ancestor role of that role can decrypt the data. It came to ssconsider that the data owners and users reside outside this role system infrastructure (where the roles are being administered). Hence the issues to consider are how the data owners can decide whether or not to trust the role managers in the system and how the role managers can decide whether and how much to trust the users in the system. Owners consider the trust of role managers in order to ensure that their data is secure after being assigned to the roles, and role managers consider the trust of users so that users with negative behaviors are excluded from the roles, which in turn makes owners trust these roles.

Owner-Role Rbac Trust Model

In owner trust models for RBAC systems it defines three entities namely, Owner, User and Role. Owner is the entity who owns the data and stores it in an encrypted form in the cloud and User is the entity who wishes to access the data from the cloud. Role is the entity that associates users with the access to owners' data, and each role manages the user membership of itself. When we refer to Role in such a context it implys role managers.

Role-User RBAC Trust Model

Since the trustworthiness of a role is primarily determined by the behaviour of users of the role, it is important for the role to ensure that only users with good behaviour are granted membership. If roles do not have a way to evaluate the trust of their users, it would be difficult for them to distinguish the malicious users from those with good behaviours. For that it uses a trust model for role's trust in users as an extension of the owner's trust model on roles. This trust model aims to assist a role to determine the trust of users who belong to the role or want to join the role. Roles can use this model to periodically check and revoke the memberships from users whose trust values are below the preset threshold. This trust model can also be used by roles to determine the trust value of a new user requesting to join.

3. PROPOSED SYSTEM

To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that data can only be accessed by those who are allowed by access policies. Many access control models have been proposed over the years in the literature. In this context, role-based access control (RBAC) is a well-known access control model which can help to simplify security management especially in large-scale systems. In the RBE scheme proposed in the paper the users management can be decentralized to individual roles; that is, the administrators only manage the roles and the relationship among them while the roles have the flexibility in specifying the user memberships themselves.

The proposed system ensures a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes along with ring signature. Ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group member's keys was used to produce the signature. A ring signature scheme is a triple of ppt algorithms (Gen, Sign, and Vrfy) that, respectively, generate keys for a user, sign a message, and verify the signature of a message. It also detects whether a data leakage has occurred or not by using the ring signature and blocks the malicious user from further accessing.

The proposed system is a signature based role access control mechanism, also known as role-oriented ring signature. In this scheme, only the person who belongs to the designated role can verify the validity of the ring signature. In role-oriented signature, nobody besides the designated role can verify the signature. Obviously, in a PKI authentication frame, each person should have his own key pair. So the core issue of role-oriented signature is how to design a scheme in which each role member is allowed to verify the signature independently. As we have mentioned above, a ring signature with limited verification range is necessary in some instances. A signer can perform following steps to produce a role-oriented ring signature.

A ring signature scheme is a triple of ppt algorithms (Gen, Sign,Vrfy) that, respectively, generate keys for a user, sign a message, and verify the signature of a message. Formally:

_ Gen(1^k), where k is a security parameter, outputs a public key PK and secret key SK.

_ Signs;SK(M;R) outputs a signature σ on the message M with respect to the ring R =

(PK1; : : : ; PKn). We assume the following:
(1) (R[s], SK) is a valid key-pair output by Gen;
(2) |R| >= 2 (since a ring signature scheme is not intended to serve as a standard signature scheme); and
(3) each public key in the ring is distinct.
The first of the above conditions simply models ring signature usage (where a signer "knows"their index s in the ring). The latter two conditions are without much loss of generality: itis easy to modify any ring signature scheme to allow signatures with |R| = 1 by including a special key for just that purpose, and given a ring R with repeated keys the signer/verifier can simply take the sub-ring of distinct keys in R and correctness (see below) will be unaffected.

_ VrfyR(M; σ) outputs a single bit indicating validity or invalidity of a purported signature _
on a message M with respect to the ring of public keys R.
It require the following correctness condition: for any k, any f(PKi; SKi)gn i=1 output by Gen(1k),any s 2 [n], and any M, we have VrfyR(M; Signs;SKs(M;R)) = 1 where R = (PK1; : : : ; PKn).

Implementation

Experience Based Trust

Trust has played a foundational role in security for a long period of time. Most experience-based trust systems derive the trustworthiness of an entity from both its own experience and the feedback on the transactions provided by other entities which have had interactions with the entity concerned in the past. Let us consider a simple example of such a system. When a client c finishes a transaction with a service provider p, c gives a feedback as either "positive" or "negative" depending on whether or not c is satisfied with the transaction. The feedback record is of the form f = (c; p; b; t) where b represents the binary value of the feedback and t is the timestamp when the transaction took place. This record f is uploaded by the client to a trust central repository.

Role-Based Access Control

Role-based access control provides a better security solution for accessing data on cloud. Roles in RBAC are based on access permissions. All users are assigned to appropriate roles and receive access permissions only through roles to which they are assigned. Typically, role-based access control model has three essential structures: users, permissions and roles. A role is a higher level representation of access control. User corresponds to real world users of the computing system. User authorization can be accomplished separately; assigning users to existing roles and assigning access privileges for users. Permission provides access to users in the system and roles describes the functions of users within an organization. In RBAC, there is a hierarchical structure; a role can inherit access permission from another role. Data owner uses cryptographic techniques to protect data from unauthorized access and the authorized users can access data. If the user satisfies the access policy, user can decrypt data by using his private key. The role based access policies are strengthened by using role-based encryption scheme (RBE).

Ring Signature

In cryptography, Ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group member's keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup.

4. SYSTEM WORKFLOW

For the successful login of a user they must get an approval from the role manager. While giving approval, a unique signature will gets generated for each role members. The Signature will be in hexadecimal format and is generated by using the Ring Signature scheme.

The Data owner can upload files in to the system. Each file which is to be uploaded is encrypted with encryption key and the signature of data user is attached along with it. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system

User requests the file by providing details and in response system replies with encrypted file. Before that the system will checks the role and signature of the users whether the receiver have the same role as the sender mentioned. It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has correct role and signature, if it's correct, the original file gets decrypted for the receiver.

There is an assumption that these role members are trusted and will not redistribute resources of the data owner to users who are not in that role. However, it is possible that a user leaks the content of a resource to others. Therefore, the data owners will need a trust system to assist them in identifying the roles which have malicious users, and hence avoid accepting the subscriptions from them. On identifying the malicious user it' s trust factor will be evaluated and if it is equal to 1 that particular user will be blocked from the role.

5. CONCLUSION

In this paper, it proposes a signature based role access control mechanism, also known as role-oriented ring signature. In this scheme, only the person who belongs to the designated role can verify the validity of the ring signature. In role-oriented signature, a unique signature is generated for each user while the role manager approves the user. By using ring signature it can detect the malicious user who performs unauthorized sharing of files. This system is efficient because it doesn't involve any certificate verification and also it considers overcoming security issues in accessing cloud information such as authentication, costing, timing for uploading of data.

Access control is found to be a significant mechanism for protecting confidentiality and privacy in cloud storage. The malicious user who shares the files to the unauthorized users of other roles can be identified by verifying the signatures. Thus the data leakage can be detected. In future it can be extended to implement methods to prevent the data leakage at the cloud server with suitable model that could reduce computation complexities at content owner, which needs continuous attention and further enhancement makes the researches in this field to get more and more intensive.

REFERENCE

1. D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in Proceedings of the 15th NIST-NCSC National Computer Security Conference. NIST, National Computer Security Center, October 10-13 1992, pp. 554 – 563.
2. Lan Zhou,Vijay Varadharajan,and Michael Hitchens "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage" IEEE Transactions on Information Forensics and Security, vol. 10, issue: 11, Page(s): 2381 – 2395, November 2015.
3. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure Role- Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947–1960, 2013.
4. Y. Zhu, H. Hu, G.-J. Ahn, H. Wang, and S.-B. Wang, "Provably secure role-based encryption with revocation mechanism," Journal of Computer Science and Technology, vol. 26, no. 4, pp. 697–
5. L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," The Computer Journal, vol. 54, no. 13, pp. 1675–1687, October 2011.
6. L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in TrustCom 2013. IEEE, July 2013, pp. 560–569.
7. M. Toahchoodee, R. Abdunabi, I. Ray, and I. Ray, "A trust-based access control model for pervasive computing applications," in DBSec 2009, ser. LNCS, vol. 5645. Springer, July 12-15 2009, pp. 307–314.
8. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "A data outsourcing architecture combining cryptography and access control," in Proceedings of CSAW 2007. ACM, November 2 2007, pp. 63–69.
9. S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in VLDB. ACM, September 23-27 2007, pp. 123– 134.
10. S. Chakraborty and I. Ray, "Trustbac - integrating trust relationships into the rbac model for access control in open systems," in SACMAT 2006. ACM, June 2006, pp. 49–58.