ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Authentication and Access Control for Cloud Computing using RBDAC Mechanism

Mali Varsha, Prof. Pramod Patil

M.E. Student, Dept. of Computer Network, Nutan Maharashta Institute of Engineering and Technology, Talegaon, Dabhade, Pune, India

Professor, Dept. of Computer Network, Nutan Maharashta Institute of Engineering and Technology, Talegaon, Dabhade, Pune, India

ABSTRACT: Conventional access control models like role based access control are suitable for regulating access to resources by known users. However, these models have often found to be inadequate for open and decentralized multi-centric systems where the user population is dynamic and the identity of all users are not known in advance Cloud computing is one of the emerging and promising field in Information Technology. It provides services to an organization over a network with the ability to scale up or down their service requirements. Cloud computing services are established and provided by a third party, who having the infrastructure. Cloud computing having number of benefits but the most organizations are worried for accepting it due to security issues and challenges having with cloud. Security requirements required at the enterprise level forces to design models that solves the organizational and distributed aspects of information usage. Such models need to present the security policies intended to protect information against unauthorized access and modification stored in a cloud. 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. In this project we are proposing trust model to improve the security for stored data in cloud. The proposed trust models provide approach for the data owner and users to determine the individual role. We present a design of a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes.

KEYWORDS:Role-based access control, data storage, role-based encryption, cloud computing, architecture.

I. INTRODUCTION

Three has been a growing trend in the recent times to store data in the cloud with the dramatic increase in the amount of digital information such as consumers' personal data to larger enterprises wanting to back up databases or store archival data. Cloud data storage can be particularly attractive for users (individuals or enterprises) with unpredictable storage demands, requiring an inexpensive storage tier or a low cost, long-term archive. By outsourcing users' data to the cloud, service providers can focus more on the design of functions to improve user experience of their services without worrying about resources to store the growing amount of data. Cloud can also provide on demand resources for storage which can help service providers to reduce their maintenance costs. Furthermore, cloud storage can provide a flexible and convenient way for users to access their data from anywhere on any device. However, several recent surveys [1], [2] show that 88% potential cloud consumers are worried about the privacy of their data, and security is often cited as the top obstacle for cloud adoption. There are different types of infrastructures associated with a cloud [3]. A public cloud is a cloud which is made available to the general public, and resources are allocated in a pay-as-you-go manner. A private cloud is an internal cloud that is built and operated by a single organisation. The organisation has full control of the private cloud, and the private cloud cannot be accessed by external parties. Hence a private cloud is often considered to be more secure and trusted. A recent survey [4] shows that nearly half, 43% of all companies report utilizing private clouds and 34% of companies say they will begin to use some form of privateCloud in the next six to twelve months.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

In this paper, we address the issue of secure data storage in the public cloud. Public cloud is formed by one or more data centres often distributed geographically in different locations. Users do not know where their data is stored and there is a strong perception that users have lost control over their data after it is uploaded to the cloud. In order to allow users to control the access to their data stored in a public cloud, suitable access control policies and mechanisms are required. The access policies must restrict data access to only those intended by the data owners. These policies need to be enforced by the cloud. In many existing cloud storage systems, data owners have to assume that the cloud providers are trusted to prevent unauthorized users from accessing their data.

II. RELATED WORK

A. ACHIEVING SECURE ROLE-BASED ACCESS CONTROL ON ENCRYPTED DATA IN CLOUD STORAGE [1]

From this paper we Refer-

In this paper, first we proposed a new RBE scheme that achieves efficient user revocation. Then we presented a RBAC based cloud storage architecture which allows an organisation to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. Then we have developed a secure cloud storage system architecture and have shown that the system has several superior characteristics such as constant size cipher text and decryption key. From our experiments, we observe that both encryption and decryption computations are efficient on the client side, and decryption time at the cloud can be reduced by having multiple processors, which is common in a cloud environment. We believe that the proposed system has the potential to be useful in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these access policies.

B. A TRUST-BASED ACCESS CONTROL MODEL FOR PERVASIVE COMPUTING APPLICATIONS [2]

From this paper we Refer-

Traditional access control models are mostly not be suitable for pervasive computing applications. Towards this end, we propose a trust based access control model as an extension of RBAC. We use the context-sensitive model of trust proposed earlier as the underlying trust model. We investigate the dependence of various entities and relations in RBAC on trust. This dependency necessitates changes in the invariants and the operations of RBAC. The configuration of the new model is formalized using graph-theoretic notation. In future, we plan to incorporate other environmental contexts, such as space and time, to our model. We also plan to investigate conflicts and redundancies among the constraint specification. Such analysis is needed before our model can be used for real world applications.

C. SECURE ROLE BASED DATA ACCESS CONTROL IN CLOUD COMPUTING [3]

From this paper we Refer-

This paper aims at fine-grained data access control in cloud computing. One challenge in this context is to achieve fine grainedness, data confidentiality, and scalability. Simultaneously, which is not provided by current work? In this paper we propose a scheme to achieve this goal by exploiting KP- ABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Formal security proofs show that our proposed scheme is secure under standard cryptographic models.

D. ACHIEVE FINE GRAINED DATA ACCESS CONTROL IN CLOUD COMPUTING USING KP-ABE ALONG-WITH LAZY AND PROXY RE-ENCRYPTION [4]

From this paper we Refer-

In this we greatly reduce the complexity of key management along with the privacy compared. Uses ABE to encrypt the data, so that users can allow access to different domains/areas with different professional roles, qualifications. We enhance an existing ABE scheme to handle efficient and on-demand user deletion/revocation, and prove its security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

E. DEVELOPING SECURE CLOUD STORAGE SYSTEM BY APPLYING AES AND RSA CRYPTOGRAPHY ALGORITHMS WITH ROLE BASED ACCESS CONTROL MODEL [5]

From this paper we Refer-

In this paper, we have addressed security issues in cryptographic role-based access control systems for securing data storage in a cloud environment. We presented a RBAC with AES and RSA based secure cloud storage system which allows an organization to upload data securely in a public cloud, while we have stored organizational information on a private cloud. The experience trust model was integrated into the SCSS.

F. DATA SECURITY FOR CLOUD STORAGE SYSTEM USING ROLE BASED ACCESS CONTROL [6]

From this paper we Refer-

Role-based encryption scheme is proposed to achieve efficient user revocation. Role-based access control model based on hybrid cloud storage architecture in which encrypted data is stored on public cloud and sensitive information related to organization stored on private cloud, from which outside users cannot access data directly. RBAC contain some privileges and access policies. Based upon authorization and access permission policies, user can access data from cloud.

G. TRUSTBAC INTEGRATING TRUST RELATIONSHIPS INTO THE RBAC MODEL FOR ACCESS CONTROL IN OPEN SYSTEMS [7]

From this paper we Refer-

In this work, we introduce the TrustBAC model for access control in open systems. The model extends the RBA model by introducing the notion of trust levels. Instead of users being assigned to roles as in traditional RBAC, users are assigned to trust levels. The user to trust level assignment is determined by three factors user's past behavior, knowledge about the user (for example, credentials presented by the user) and recommendation provided by others about the user.

III. PROPOSED SYSTEM

The proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. 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 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.The paper has proposed trust models for owners and roles in RBAC systems which are using cryptographic RBAC schemes to secure stored data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

IV. SYSTEM ARCHITECTURE

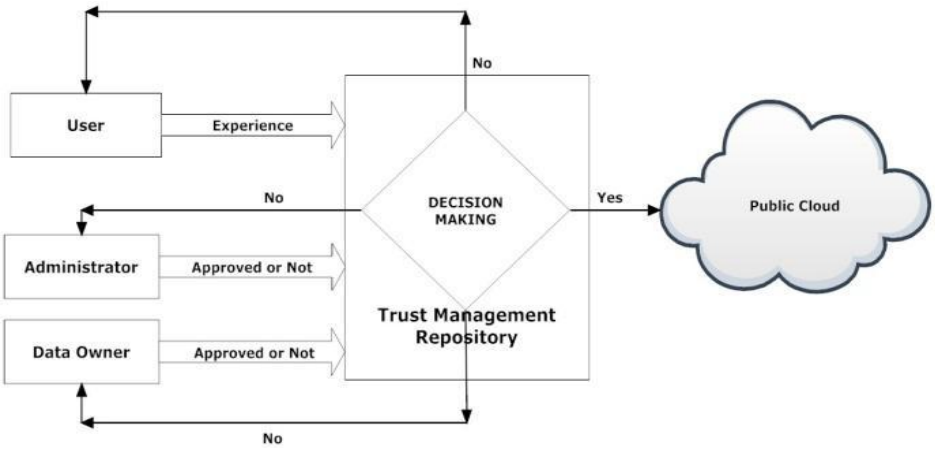

Fig1: System Architecture

Explanation

All the required algorithms in the RBE scheme have been executed properly to setup the system parameters. We first look at the case where an owner wants to encrypt a message M to the role R3. The inputs of the RBE encryption are the system public keys pk and the role public parameters pubR3 of R3, and the output of the algorithm is the cipher text tulle.

RBE decryption algorithm to recover the message M, and the inputs of the algorithm are pk, the role public parameters pub R1 the user decryption key dkU1 and the cipher text C. The algorithm outputs the message M if the decryption key dkU1 that U1 holds is valid.

Trust issues that need to be considered by the data owners and role managers of a cryptographic RBAC system.

V. MODULES DESCRIPTION

A. 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 thepast. 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.

B. Role-based Encryption

A cryptographic RBAC scheme integrates encryption scheme with RBAC model to enforce the access control policies in an entrusted environment. This approach allows data to be encrypted in the way that the cipher text can only be decrypted by those which are allowed by the access policies. A hierarchical cryptographic access control scheme was proposed in 1983. Because of the similarity in structures between hierarchical access control and RBAC, a hierarchical cryptographic access control scheme can be easily transformed into a cryptographic RBAC scheme. The problem of access control for securely outsourcing data using cryptographic techniques was first considered in. Several cryptographic access control approaches have been investigated in to address the problem of secure data access and cost effective key management in distributed environments. Among the cryptographic RBAC schemes in the literature, role-based encryption (RBE) schemes have achieved many superior characteristics compared to other solutions in terms of efficiency and flexibility.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

C. Trust issues in using cryptographic RBAC schemes in secure cloud storage

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. In this paper, we assume 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 make owners trust these roles. In this section, we discuss the trust issues that need to be considered by the data owners and role managers of a cryptographic RBAC system.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have addressed trust issues in cryptographic RBAC systems for securing data storage in a cloud environment. The paper has proposed trust models for ownersand roles in RBAC systems which are using cryptographic
RBAC schemes to secure stored data. These trust models assist owners and roles to create flexible access policies, and cryptographic RBAC schemes ensure that these policies are enforced in the cloud. The trust models enable the owners and roles to determine the trustworthiness of individual roles and users in the RBAC system respectively. They allow the data owners to use the trust evaluation to decide whether or not to store their encrypted data in the cloud for a particular role. The models also enable the role managers to use the trust evaluation in their decision to grant the membership to a particular user. Another significant contribution of this paper is that the proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. As far as we are aware, this is the first time such a trust model for role-based access control system taking into account role inheritance has been proposed. We designed the architecture of a trust-based cloud storage system which has shown how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also described the application of the trust models by considering a practical scenario and illustrating how the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and role managers of the cloud storage service.

REFERENCES

[1] Lanzhou “achieving secure role-based access control on encrypted data in cloud storage” ieee transactions on information forensics and security, vol. 8, no. 12, december 2013
[2] Manachaitoahchoodee” a trust-based access control model for pervasive computing applications” u.s.afosr under contract fa9550-07-1-0042
[3] V.sathyapreiya “secure role based data access control in cloud computing” international journal of computer trends and technology- may to june issue 2011
[4] Hulawalekalyani” achieve fine grained data access control in cloud computing using kp-abe along-with lazy and proxy re-encryption” international journal of emerging technology and advanced engineering volume 4, issue 2, february 2014)
[5] Bokefodejayant d.” Developing secure cloud storage system by applying aes and rsa cryptography algorithms with role based access control model” international journal of computer applications (0975 – 8887) volume 118– no.12, may 2015
[6] Prachi shah” data security for cloud storage system using role based access control” international journal of science and research (ijsr) issn (online): 2319-7064 index copernicus value (2013): 6.14 | impact factor (2013): 4.438
[7] Sudipchakraborty” trustbac integrating trust relationships into the rbac model for access control in open systems” sacmat’06, june 7–9, 2006, lake tahoe, california, usa.