ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10, December 2012

Reputation Management in Distributed Community Clouds

Anupriya koneru[1], Dr K. Venugopal Rao[2]

Assistant Professor, Department of Information Technology, LBRCE, Mylavaram, India[1]

Professor & HOD, Department of Computer science and Engineering, GNIT, Hyderabad, India[2]

ABSTRACT: **Two or more community clouds are going to form as a group called network to provide services to satisfy the organizational needs. It works in the distributed environment. While communicating a cloud with other cloud in the group, it has to be sure that the other cloud is a good cloud; otherwise it won't perform any transaction with that cloud. To know that in this paper we are going to present a protocol which provides the reputation of the cloud and a root certification for identity management. By omitting such bad transactions we can reduce number of malicious activities in the cloud computing.**

Keywords: cloud computing, community clouds, reputation, distributed systems security, root certification.

I. INTRODUCTION

The clouds in the group have to be discouraged from leeching on the network. It has been shown in Tragedy of commons [1] that a system where peers work only for selfish interests while breaking the rules decays to death. Securing these groups is extremely difficult due to the decentralized nature of these distributed networks.

The traditional techniques developed for the centralized systems cannot be used for distributed systems. This is because the absence of central authority. The disadvantage of the centralized approach is, if the central authority turns malicious, the total group will become vulnerable which affects the security of organizations that has used services from this group.

In this paper, we investigate Reputation systems for distributed community clouds network – a more ambitious approach to protect the network without using central component, and there by providing the full benefits to the organizations whoever are requesting services of these groups.

The reputations of the clouds are used to determine whether a cloud is a malicious are good in the network. Once detected, the malicious clouds are exclude .from the network as the good clouds do not perform any transactions with the malicious clouds.

All the clouds in the distributed community clouds network are identified by identity certificates. The reputation of a given cloud is attached to its identity. The identity certificates are generated using root certification; all clouds maintain their own certificate authority which issues the identity certificates to the cloud. Each cloud owns the reputation information for all its past transactions with other clouds in the network, and stores it locally.

II. RELATED WORK

A. Cloud computing

Today, the latest paradigm to emerge is that of Cloud computing [2] which promises reliable services delivered through next-generation data centres that are built on compute and storage virtualization technologies. Consumers will be able to access applications and data from a "Cloud" anywhere in the world on demand. In other words, the Cloud appears to be a single point of access for all the computing needs of consumers. The consumers are assured that the Cloud infrastructure is very robust and will always be available at any time. The main advantages of a cloud are Low cost, Mobility, Works on different platforms, Security and confidentiality and Storage space. It is able to scale rapidly, store information remotely and share services in a dynamic environment which can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. The traditional mechanisms for privacy are no longer flexible or dynamic enough, so new approaches need to be developed to fit this new paradigm.

B. Community cloud

A community cloud [3] in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10, December 2012

concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

C. Distributed systems security

In this section, we review some of the solutions developed for protecting the users of distributed community clouds using distributed CAs. This section is focused on distributed systems components.

1) SDSI: SDSI [4] is a Simple Distributed Security Infrastructure, simplifies the X.509 certificates design and provides the means for self-certification, local name spaces, secure formation of groups, and simple access control mechanisms. It also provides methods to incorporate global name spaces and globally trusted identities within the SDSI infrastructure. In SDSI, the "authority" is distributed among all members of the networks.

2) Dynamic Trust Management: Dynamic Trust Management [5] encapsulates trust management in dynamic distributed environments, where the members of the system assume frequently changing multiple roles.

3) RBAC: Role-Based Access Control was introduced in 1992 by Ferraiolo and Kuhn [6]. RBAC associates permissions with roles and not with users. The users are assigned roles in a many-to-many relationship, i.e., one user can have many roles and vice versa.

D. Cryptographic blinding

Cryptographic blinding was introduced by Chaum in 1983 [7]. Cryptographic blinding enables an authority to digitally sign on a document without seeing the content of the document.

E. Security in clouds

Security in cloud computing [8] is a wide range of technology. It established controls to protect companies' information, applications and related infrastructures to cloud computing. All security problems in internet are present in clouds too because of service providing by internet. In Cloud computing also we are using same protocols and security frameworks but they are not context oriented, so they need a powerful set of security protocols to transfer data safely.

F. Security in community clouds

The community cloud raises the question of how providers authenticate consumers, qualify them for service, and hold them accountable for their actions in the cloud. A user's privilege at a provider is based on membership in organizations, roles and status within organizations, and relationships and agreements among organizations and providers, and community policies and provider policies for authorization and resource management. These affiliations, roles, relationships, and policies may change frequently.

III. REPUTATION SYSTEM IN CLOUDS

A. Root Certification of clouds

In order to participate in the reputation system, a cloud needs to have an identity. A cloud receives a recommendation for each transaction performed by it, and all of its recommendations are accumulated together for calculation of the reputation of a given cloud.

The cloud is denoted by C while the authority is denoted by A. Here C→A: X denotes that the cloud (C) sends a message X to the authority (A). The symbol PK2 represents the private key of the Cloud and PK1 represents the public key of the Cloud. EK(⌐) represents encryption of the phrase (⌐)with key K, while EBK (X) represents blinding phrase X with key K.

- C→A: B1 = {EB ka (I Alice r)}, I Alice

The Cloud Alice generates a BLINDING KEY, Ka and another identity for herself (I Alice r). Alice cannot be identified from her identity (I Alice r). Subsequently, she blinds her identity (I Alice r) with the blinding key Ka. B1 represents the blinded identity. Alice sends B1 to the authority with her real identity that proves her membership to a group.

- A→C: B2 =E p Authorityk2 {B1 = {EB ka (I Alice r)}

The authority signs the blinded identity, B1 and sends it (B2) back to the Cloud.

- C: E p Authorityk2 {I Alice r} = {EB ka {B2}}

The Cloud unbinds the signed identity and extracts the identity Authorized by the authority E p Authorityk2 {I Alice r}.

B. Model

In network once a cloud has obtained its identity, it joins the distributed community clouds network using the standard Join method. The cloud (requester) searches for one or more files using the Search method provided by the network. On the basis of the responses received, as a result of its search request, the requester generates a list of clouds that have the requested file(s). The number of clouds who offer a particular file is denoted by RANGE. The requester selects the cloud (provider) with the highest

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10, December 2012

reputation from the list and initiates the cryptographic protocol. If the requester is a trusted cloud then only it will transfer the actual Text file. The reputation protocol is presented in detail in the next section. In the protocol, the requester uses the Download method of the network, to download the file from the provider. Subsequently, it verifies the integrity, authenticity, and the quality of the file. Depending on its verification results, it sends a recommendation between MIN_RECOMMENDATION and MAX_RECOMMENDATION to the provider. Once the provider receives the recommendation, it averages the previous recommendations received by it and the recent recommendation to calculate its reputation. The above mentioned steps are repeated for every transaction.

IV. CLOUD REPUTATION PROTOCOL

Once the requester cloud has selected the provider with the highest reputation, it initiates the cloud reputation protocol with the provider. In the Cloud Reputation protocol, the requester is denoted by Rc while the provider is denoted by Pc.

Step 1: Rc→Pc: RTS & IDR

The requester cloud sends the request and identity of the requester cloud to the provider.

Step 2: Pc→Rc: IDP & TID & EPK2 (H(TID ‖ RTS))

The provider sends its own id, transaction id and signed transaction id.

This signed transaction id is required to ensure that the provider cloud does not use this same TID again.

Step 3: Rc: LTID = Max (Search (PK1 ‖ TID))

Requester cloud verifies the last transaction id of the provider by searching in the network.

Step 4: Rc: IF(LTID ⩾ TID) GO TO Step 12

By obtaining the LTID, it verifies whether the LTID is less than the new TID.

If so it indicates the new TID was not used in any other transactions of the provider cloud.

Else, it indicates the provider cloud is going to play a foul, jump to 12

Step 5: Rc→Pc: Past Recommendation Request & r

The requester cloud is sending a request for the provider's previous recommendations till r transactions.

Step 6: Pc→Rc: SEQUENCE, EPK2 (SEQUENCE)

SEQUENCE = ({RECN-1 ‖EZN-1K2 (H(REC N-1)}‖{RECN-2‖EZN-2K2(H(RECN-2,RECN-1))}‖{RECN-3‖EZN-3K2(H(RECN-3,RECN-2))}‖{RECN-4 ‖EZN-4K2(H(RECN-r,RECN-r-1))})

The provider sends the sequence.

Step 7: Rc : Result =V erify(REC N-1,RECN-2 . . .RECN-r)

If Result != Verified GO TO STEP 12

Step 8: Pc→Rc: File or Service

After verification, the file or service is transferred from the provider cloud to the requester.

Step 9: R c→P c: B1 = EBKa(REC ‖ TID ‖ ERK2{H(REC, ‖ TID)})

After verifying the quality, integrity and authenticity of the file, it provides a recommendation by using blinding key.

Step 10:

a. Pc →Rc: B1 ‖ EPK2 (H(B1), nonce),nonce

The provider cloud can not see the recommendation given by the requester because it does not have the blinding key. So, it simply sign's on that.

Whatever recommendation has been given by the requester that should be accepted by the provider cloud.

b. Rc→Pc: Ka

Now the requester cloud sends blinding key to the provider.

Step 11: Insert (IDR; {REC ‖ TID ‖ ERK2{H(REC) ‖ H(TID)}})

By using that blinding key, the provider will see the recommendation given by requester.

This will be inserted into the network for calculating the reputation.

Step 12: Step 12 explains the steps a requester executes when it expects foul play: ABORT PROTOCOL

Rc: Insert (IDR, {SEQUENCE ‖ TID ‖ ERK2{H(SEQUENCE) ‖ H(TID)}}) .

IV. FEATURES OF REPUTATION MANAGEMENT IN CLOUDS

The provider cloud is accountable for all its previous transactions. The provider cannot modify any recommendation because they are already digitally signed by the requesters.

The requester cloud cannot maliciously abort the transaction after receiving a file without giving recommendation. If it does so, the provider cloud will get max recommendation.

- Raising quality and improving the flexibility
- Securing cost savings and sustainable efficiencies through economies of scale.
- Release of staff time from 'commodity' activities for more added-value/customer-facing activities.
- Improving the scalability of systems.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10, December 2012

- Ensuring improved and more up-to-date systems.
- Gaining competitive advantage.
- Ability to offer otherwise unsustainable services.
- Levering transformation.
- Improved cooperation with other institutions enabling strategic development of cross-institution support services.
- Reducing the environmental impact of IT activities.
- Addressing growing demand for collaborative learning & teaching, research and knowledge exchange.

VI CONCLUSION

In this paper we have seen security considerations in community cloud communication by providing root certification and reputation based protocols. Currently the reputation of the provider cloud is considered and reputation of the requester is ignored. This can be extended to encapsulate the reputation of both provider and requester clouds.

VII ACKNOWLEDGMENT

I am heartily thankful to my guide, Dr Venugopal Rao, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of the paper.

REFERENCES

[1] H. Garett, "Tragedy of Commons," Science, vol. 162, pp. 1243-1248, 1968.
[2] Yasaman Mirfakhrai, Mehran Mohsenzadeh, Seyed Mohsen Hashem, Proposing an Interoperable Framework among Cloud Providers, Volume 55/Number 11 ISBN: 973-93-80870-90-9.
[3] Je Chase, Prateek Jaipuria Department of Computer Science Duke University Steve Schwab and Ted Faber USC/ISI "Managing Identity and Authorization for Community Clouds "August 21, 2012 Technical Report CS-2012-08.
[4] R.L. Rivest and B. Lampson, "SDSI: A Simple Distributed Security Infrastructure," Proc. Crypto '96, pp. 104-109, Aug. 1996.
[5] N. Li and J.C. Mitchell, "RT: A Role-Based Trust-Management Framework," Proc. Third DARPA Information Survivability Conf. and Exposition (DISCEX III), Apr. 2003.
[6] D. Ferraiolo and R. Kuhn, "Role-Based Access Controls," Proc.15th Nat'l Computer Security Conf., May 1992.
[7] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Advances in Cryptology (Crypto '82), 1983.
[8] Farhad Soleimanian Gharehchopogh, Sajjad Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", International journal of scientific and technology research volume1, ISSUE 6, JULY 2012 ISSN 2277-8616.

Biography

K. Anupriya is currently working as an Assistant Professor of IT in Lakireddy Bali Reddy College of Engineering, Mylavaram, India. She received her M.Tech degree from JNTU Vijayanagaram University, Vijayanagaram, in 2011.