Survey on Establishing Trust, Data Security and Authentication In Hybrid Cloud Computing

Mr. Mithil P. Gharat
Dept. Of Computer Engineering
Vidyalankar Institute of Technology
Mumbai,India

Prof. Dilip Motwani
Dept. Of Computer Engineering
Vidyalankar Institute of Technology
Mumbai,India

***Abstract*—With the Progress in cloud computing technology, the social demand for cloud computing is growing that also increases demand for data security especially in hybrid model. Also when its scope enlarges to ubiquitous and pervasive computing there will be need to maintain trustworthiness. Numerous Techniques have been developed for data security and authentication and purpose of this paper is to categorize and evaluate these methods. For managing trust includes Feedback management approach will be discussed. Paper Also Summarizes several methods to protect data which includes Single Encryption, Multi-level Virtualization and Authentication Interface ,Also Authentication including Several scenarios.**

***Keywords*— hybrid cloud environment, private clouds, public clouds, trust model, cloud computing, security of data, data privacy, authorization, user trust**

I. Introduction

Cloud Computing is a new distributed paradigm for on demand and dynamic provisioning of computing resources to potential end users and leveraging virtualization and internet technologies .Cloud computing Classified into Public Private and Hybrid models.

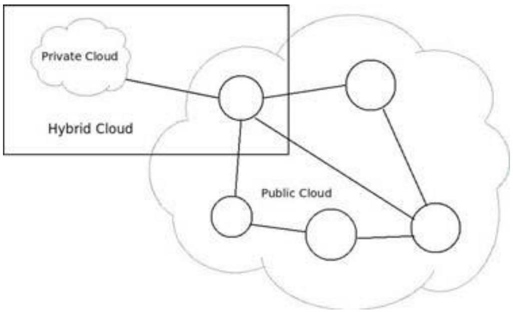

Fig. 1 Hybrid Cloud Computing Model.

Hybrid cloud computing model provides a greater flexibility: private cloud part can guarantee the safety of the user's data; public cloud can provide users with good scalability. Thus it is important to maintain a trust management system that permits one to distinguish the trustable from the non-trustable participants in a hybrid cloud model. Although, it has been clearly shown that an assurance of a higher degree of trust relationship is required to attain efficient resource allocation and utilization, to the best of our knowledge, the problem of how to determine service trustworthiness in hybrid cloud computing environments has not been addressed in a satisfactory manner.

II. Establishing Trust in Hybrid Cloud

A. *Trust Management Framework*

Cloud providers provide resources and services to potential users for fee or following another economic model such as bartering. Resource providers have their cost structures and policies that govern how their resources are provisioned to a user.

IJERT

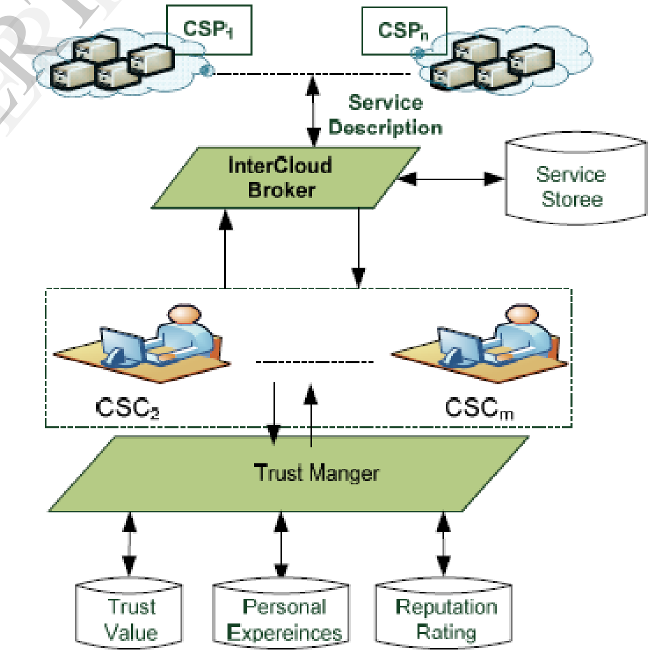

Fig.2 The Hybrid Cloud Computing Architecture.

- *Cloud Resource Manager*
  Users submit their resource allocation requests to their local Cloud Resource Manager (CRM). The CRM is responsible for the resource provisioning and al location at the individual cloud level.

- *Inter Cloud Broker*
  The inter cloud broker (ICB) is responsible for mediating the resource exchange between peering clouds. ICB also provides external cloud selection capabilities by selecting suitable clouds that are able to provide the required resources to users' requests. It is also responsible for managing requests for resources and services from other cloud ICBs. In addition, ICB is also responsible for monitoring the execution of applications across multiple clouds. The ICB also interacts with other entities including accounting systems that provide information on shares consumed by peering clouds.

- *Trust Manager*
  It is responsible for getting the user's feedback, verifying the user's feedback and updating the same value in the feedback repository. we specify trust in the form of a trust relationship between two peering entities, Personal experiences and reputation rating. service reputation rating and personal experiences are separately updated after a transaction.

B. *Feedback Management Approach*

Two algorithms have been developed to determine a user's trust value based on a sequence of her interactions and past behaviors

- *Personal experiences*
  They represent the first hand information of ***u*** after transacting with ***w*** . Personal experiences are represented as

  $P_{u,w}$=(k, $S_{u,w}$)   (1)

  where $S_{u,w}$ denotes the personal satisfaction of ***u*** regarding based on the quality of service in the k$_{th}$ transaction. Personal experiences are shared with the members of the peering group in the form of personal satisfaction feedback. When no experience with a service is made in a long time, the aged trust relationship might no longer be valid.This usually means that the trust confidence level decreases over time which will be denoted by fading factor. The fading factor is defined as a function of the number of successful transactions that service customer and the service providers had engaged in prior to computing the feedback

- *Feedback filtering approach*
  Each cloud,upon request or periodically, provides feedback about the subjective quality of a received service from a given cloud provider, The metrics used to rate the quality of a service is a real number in the interval of [0, 1].A perfect service is rated with 1 while 0 indicates a completely unsatisfactory one.

  The basic principle of the proposed approach is to use the personalized similarity measure to compute the credibility of feedback through personalized experience and a variable tolerance threshold. Cloud customer's overall reputation score is outside the threshold value then that rater's ratings will be discarded from the set of ratings that contribute to the Cloud customer's score.

III. Protection Of Data security

Hybrid cloud could provide both security and the scalability at the same time. However, there still are some problems about the data security because when user extends their application to the public cloud, the cloud computing provider could access the users privacy data . There are some methods to protect users data on the public cloud.

C. *Single Enryption*

We can trust our private cloud totally and public cloud conditionally .So Encryption is required only when transfer of data from private cloud to public cloud is performed.

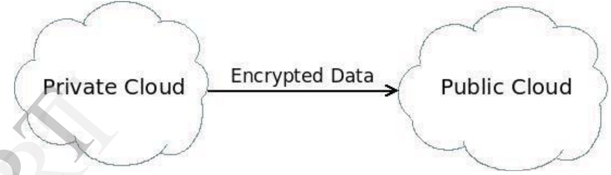

Fig.3 Single Enryption

IJERT

D. *Multi-levelVirtualization*

The improved multi-level virtualization model added another layer of run-time environment.

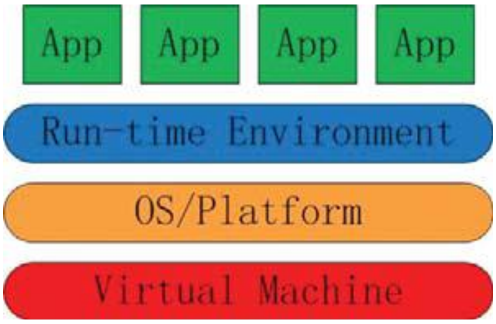

Fig.3 Multi-Level Virtualization model

The extra run-time environment could provide the capacity to control the permission to access the users data. this permission control should be independent from the cloud platform management system of cloud computing provider.

E. *Authentication interface*

In order to find the balance of the performance and the security, some applications would not need the permission control, so the case-based permission control is a better choice.

Authentication interface is integrated in the users applications, when the application running on the public cloud wish to access the data owned by hybrid cloud application (host application), it would sent permission request to the host application, host application would check the authorize list, if the request application is already authorized, the host application will give it permission to the data. And if the request application is not already forbidden, the host application would send the request back to private cloud to let the user to decide whether authorize the request or not.

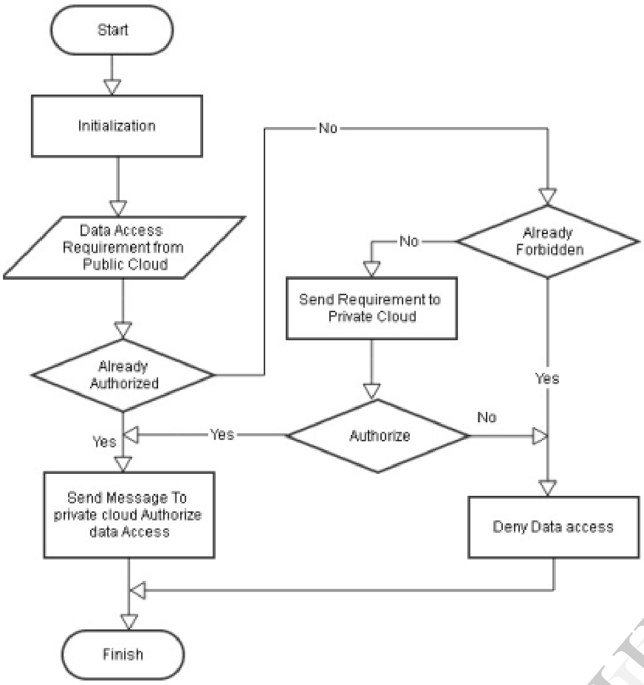
Start
Initialization
Data Access Requirement from Public Cloud
Already Authorized
Yes
Send Message To private cloud Authorize data Access
Finish
No
Already Forbidden
No
Send Requirement to Private Cloud
Authorize
Yes
No
Yes
Deny Data access

Fig 4 Authorize Flow Diagram

IV. Authentication Model

Authentication is most important aspect of securing access we will see models based on CA system.

F. *An Improvement of Secret Share*

In order to increase the security of the authentication, the private cloud would send a secret message to CA while sending the authentication request. The CA would check the trust list to find whether the public cloud provider is trustable or not.

If the provider could be trusted, the CA would send it the request from the private cloud and the secret, meanwhile the CA would also send the private cloud the public cloud provider ID. Then the provider would send the private cloud its ID and the message from CA.

The private cloud will check the ID and the message. If all of them are right, the public cloud provider could be trusted.

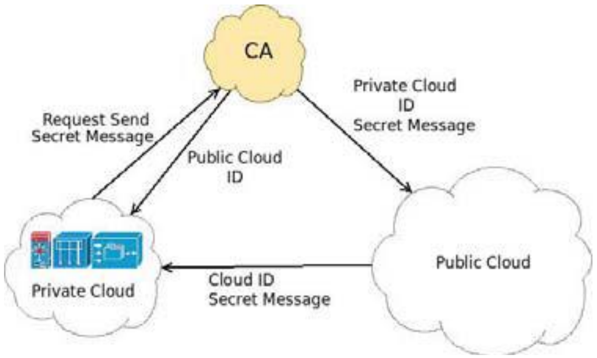

Fig 5 Secret Share Authentication Model

G. *The Generalization of The Authentication Model*

Sometimes the cloud cannot find a CA to authenticate the other cloud provider then this Generalization can be used.

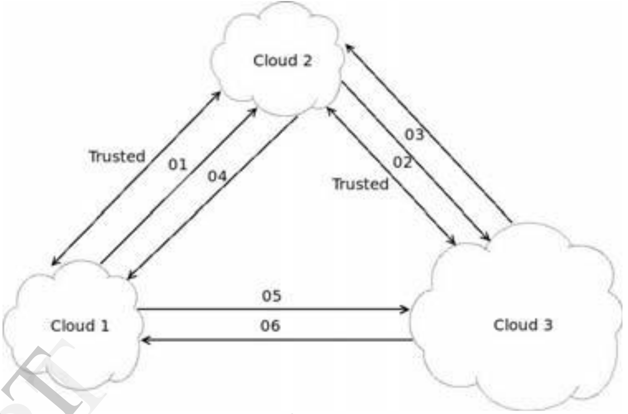

Fig 5 Generalization of Authentication Model

IJERT

In figure 5, there is a scenario that cloud 1 is already trust cloud2, and cloud 2 is already trust cloud 3. Now cloud 1 wishes to extend its computing capacity via connect another cloud. Then it can proceed in sequence shown in the figure 5 and Cloud 3 can be trusted by cloud 1 in the absence of CA.

H. *CA After System Crash.*

The cloud providers need to take measures to keep the cloud system availability even after the CA system being Crashed.

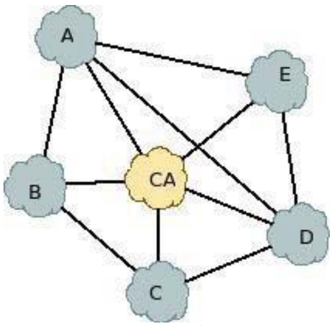

Fig 6 CA System of the Cloud Provider.

Cloud CA is the root of the cloud system, and all other public cloud are connected to the CA cloud for authentication services. If the CA cloud is not available, the other public cloud would use the saved authentication information to provide services.

If the information about required cloud is not present then that cloud will check with other clouds to get the information. Cloud having information about requested cloud will return requestor cloud. And that information will be stored by the requestor.

V. Conclusion

I. Establishing Trust

The feedback filtering approach in trust management system is reliable as it helps clouds to defend themselves against malicious information, including rating values propagated by other clouds into the system.

Trust value storage is distributed at the levels of the clouds in the system, which enables each cloud to make independent local decision for selection about trustworthiness of a cloud. Based on the trust management framework feedback filtering mechanism that can effectively address strategic feedbacks and mitigate unfairness

The quality of a reputation system depends on the integrity of the feedback ratings it receives as input. Therefore, effective protection against unfair ratings is a basic requirement and is an integral part of a robust reputation system.

II. Data Security

The single encryption is easy to achieve, yet the data is encrypted, the applications on public cloud would be difficult to reuse the data, cannot to be mined.

Multi-level virtualization contains a run-time environment level; it would cause performance loss and increase the complexity of the system. Therefore Multi-level virtualization model is suit for the scenario that all users applications need the permission control.

Authentication interface is a simple solution, and its also effective when users combined PaaS providers and SaaS providers. And it also meets the same problem like the multilevel virtualization, standardization of the interface.

III. Authentication

User authentication and directory services will be needed anywhere that employees or other users expect to access organization resources. Since some governments have strict rules about the locations of private data, try to determine where the authoritative data will reside and how it will be migrated to the other clouds that need it.

Access control and data leak prevention will become more difficult as data migrates to the cloud. As a goal, a role-based access control mechanism base on SAML claims seems to be the best bet today for providing the required functionality.

REFERENCES

[1] J. Abawajy, “Establishing trust in hybrid cloud computing environments,” in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, nov. 2011, pp. 118 –125.

[2] Jingxin K. Wang and Xinpei Jia, “ Data Security and Authentication in Hybrid Cloud Computing”, *2012 IEEE Global High Tech Congress on Electronics*

[3] A. Bhardwaj and V. Kumar, “Cloud security assessment and identity management,” in *Computer and Information Technology (ICCIT), 2011 14th International Conference on*, dec. 2011, pp. 387 –392.

[4] D. Chen and H. Zhao, “Data security and privacy protection issues in cloud computing,” in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol. 1, march 2012, pp. 647 –651.

[5] B. Gowrigolla, S. Sivaji, and M. Masillamani, “Design and auditing of cloud computing security,” in *Information and Automation for Sustainability (ICIAFs), 2010 5th International Conference on*, dec. 2010, pp. 292 –297.

[6] K. Khan and Q. Malluhi, “Establishing trust in cloud computing,” *IT Professional*, vol. 12, no. 5, pp. 20 –27, sept.-oct. 2010.

[7] A. Kim, J. McDermott, and M. Kang, “Security and architectural issues for national security cloud computing,” in *Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on*, june 2010, pp. 21 –25.

[8] S.-H. Na, J.-Y. Park, and E.-N. Huh, “Personal cloud computing security framework,” in *Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific*, dec. 2010, pp. 671 –675.

IJERT