Extension of the Trusted Cloud Domain for the Composite Cloud Process

Sameer Rajan
Govt. of India | MCIT | DIT
National Informatics Centre (NIC)
Naharlagun, Arunachal Pradesh (India)
sameer.rajan@nic.in

Apurva Jairath
Department of C.S. & Engg.
Gyan Ganga Institute of Technology & Sciences (GGITS)
Jabalpur, Madhya Pradesh (India)
apurvajairathit@gmail.com

Abstract -- Internet is a "network of networks" that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. Cloud computing [1] is a new flavor of computing where our trend of using internet changes. It makes a virtual pool of resources such as storage, CPU, networks and memory to fulfill the user's resource requirement and provides on demand (pay per use) hardware and software services without barriers. It can be named as dynamic computing because it provides resources, when required. Cloud Computing manages the pool of resources automatically and dynamically through software and hardware. Various businesses form their cloud for the users to provide pay per use services. Users are required to access the cloud according to the service. In this way, user can get benefited from the proprietary cloud on cheap prices but it is difficult for the user to find the cloud that can fulfill his demand. It is also not safe for cloud to cloud communication without trust. To resolve such difficulties and various other issues, it is required to extend the trusted cloud domain for accessing the compatible services provided by other clouds.

Keywords: Cloud Computing, Proprietary cloud, Cloud Services domain, Trust.

I. Introduction

Cloud Computing is the pool of services which provides faster, cheaper, scalable and optimized services to the users. These services include storage, processing power, memory and software service etc. Normal desktop or laptop can offer limited services. For example [1], if user wants to store images, videos, documents in limited storage and also he wants to install heavy software but if computer has limited hard disk space and memory configuration, then these tasks may not be supported by these computers. Data mining [2] applications can be a good example because some data mining applications process huge data to find out useful pattern of information. So it may require more resources to process huge data as fast as possible. In that case you are required to increase your computing power, storage capacity and also the memory size. Also, we need to purchase licensed software to do our tasks. So the users are restricted because of limited hardware and software configuration. Cloud computing can put restriction on these barriers. Cloud services are provided by many organizations. The domain of cloud services is specific to the organization. Organizations may offer services as Software as a Service, Platform as a Service and Infrastructure as a Service. A cloud may also access to the other cloud services to fulfill the user's demand.

To offer cloud services, it is required to include functional and non-functional parameters. These factors may be performance, interface, transparency, security and other functional and non-functional factors which are emphasized more, trust is one of them. Various organizations may form their own clouds according to the services like storage, computing power, memory, software. These cloud services may be accessed from intra-cloud service domain or inter-cloud service domain. A cloud service domain is an association of services with a trust broker. Trust broker provides the trust facility. Trust is a relationship of reliance.

It can happen that the required service is not available within the accessed cloud. We can say that, the required services are not inside the cloud or better services are found outside the specified cloud. But these services can't

be involved directly because these are outside the secure cloud domain. Due to some security aspects like confidentiality, integrity, access control, denial of services etc. these services can not be accessed directly from other cloud. To resolve such issues, the extension of trusted region of cloud comes in light. So to approach the required service, if it is not present in the same cloud domain, domain of trust should be extended. It may be possible by exchanging security token among domains of cloud.

Users want to access required services while it does not present in a single cloud domain. Organizations or Businesses establish their own domain of trust by exchanging tokens among a set of cloud services which are used to form the composite business process. There may be a compatible service which is better service in other domain of trust. Therefore it is required to extend the cloud domain of trust to the services which are part of a different domain of trust.

Trust Importance

Trust is the necessary for the following:

- Feeling able to rely upon another entity
- Cooperating as a group
- Taking thoughtful risks
- Experiencing believable communication
- Avoiding contention among entities.

Trust helps to provide a controlled access to shared resources in a resource domain (the trusting domain) by verifying that the incoming authentication requests is coming from a trusted authority (the trusted domain). In this way, trust act as bridge that allows only validated authentication requests to travel between domains.

As cloud services are offered through Internet, they need to be secured. A cloud services domain of trust is an association of cloud services with a trust broker. There are two types of domain trust: intra-domain and inter-domain.

Intra-domain trust

Intra-domain trust of services is needed to provide secure accessing of services within the domain. All the services are registered with the trust broker of the cloud domain. And this trust broker is responsible for providing authenticated and authorized way to access the services within the domain.

Inter-domain trust

It may happen that the required cloud services are not present in the same domain. Then, it might be accessed from other cloud services domains so it is required that the other domain must form a trusted relationship with this domain. Security is an important issue when these services exist on the Internet. Organizations may form domains of trusted cloud services by exchanging tokens among them to form a composite cloud process of compatible services.

II. Background

Nowadays, Cloud computing has become the latest trend of internet. Many organizations are trying to set up their clouds for the commercial, economical, educational, political growth.

The credit of inception of the computing era goes to mainframe computer. [1] These computers are early computers; they have large cabinet to house CPUs and memory to work. It was not financially feasible for any individual while it was used by large organizations to process the bulk data. Personal computers replace the mainframe computers, they focus on individuals. Operating on these computers is simple.
Personal computers reduce the cost, if an organization implements an application within the organization. To achieve this, it is required to have database and application interface on each individual computer. It can not only increase the cost of implementing application but also make the implementation task complex and less manageable.

Such implementation complexity can be resolved by Client- Server Computing. Server and Clients are the different entities. Server entity handles the database part while Client entity handles the interface part of the application. Client Server Computing reduces the computing cost, increases the performance, easy maintainability, scalable, highly available computing. It is also associated with the limitation of resources. This limitation restricts the client server computing and it can't be applied globally to share information in effective and efficient way. The triple 'W' (WWW) resolves such issues. WWW was founded by Tim Berners- Lee. The web is a system of interlinked hypertext documents which are accessed by internet. Internet is free from various restrictions. It has no single point of control, no single point of information, no single owner, no single user or service provider. Internet was incepted for military purpose but today it becomes the necessary part of our

modus vivendi. It provides information in distributed manner. Information or data are stored on different servers which are provided to the user when demand comes. This system also has some limitation like limitation of storage, memory and processor etc. From this point, Cloud Computing comes into picture. Cloud computing doesn't limit to grid, parallel [3] and distributed computing [4]. Cloud computing can involve power of such paradigms at any level to form a resource pool. Cloud computing offers services to the users on demand (pay per use) basis. Different clouds provide different services like Infrastructure, Platform, Software services to the interested user's group.

There are various services exist within a proprietary cloud domain but sometimes it happens that all the required services don't exist within a cloud domain while they exist out of that cloud. So, it is required to extend the cloud domain of services to other cloud domain to reach the compatible requested cloud services. The payment of services may be handled by both cloud organization internally.

Trust extension plays a critical role to smooth collaboration among cloud services from different trust domains and information sharing between trust domains. The collaboration of these cloud services makes new demands for managing trust-related behavior.

[5] suggests that a explore requirements for a federated trust management system from four aspects, and then examine a set of suitable criteria for evaluation of such a system. The purpose of this paper is not to suggest a complete set of evaluation metrics covering all necessary features; instead, its purpose is to initiate a discussion and to offer a context in which to evaluate current and future solutions, in order to encourage the development of proper models and systems for trust management.

A method to establish a dynamic trust is described in [6]. A client send request to register a trust primitive corresponding to the policy from service provides. Client's STS registers the primitive in the attribute service. The client embeds the token and sends the requests. Then service provider verifies it by asking its own STS. Both STS communicate and then request would be verified. In [7], approximately same method of [6] has been followed to establish the trust. Trust information is needed to be sent with security. In [8], a framework is proposed which is called as token exchange service (TES), which provides a set of services to make trust information exchange facilitate using security tokens. In these ways, a trusted domain of clouds may be form by exchanging tokens among the clouds which are used to form a composite cloud process.

III. Problem Statement

User wants to access any service so he has to access appropriate cloud which may offer requested service. If service is available in that cloud, user gets the service otherwise he has to search the proper cloud which may fulfill user's wish. Literally, a composite cloud process is collaboration of atomic cloud services to achieve a predefined objective. Security is an important issue while accessing these services from the internet. Thus, the cloud services collaborating to form a composite service need to be trusted. Many businesses establish their own cloud domain of trust by exchanging tokens among a set of cloud services which are used to form the composite cloud process. It may happen that more useful compatible cloud services in other domains of trust are available which may be useful in the situation when a service from the trust domain of cloud is unavailable for any reason or better non functional offerings are made by other cloud service providers. These cloud services from other domains of trust cannot be included in the composite service because of lack of trust. Therefore, it is demanded to extend the trusted domain of cloud to the services which are part of a different trusted cloud domain.

IV. Solving Approach

It is needed to extend the domain of trust to the services which are found in the different trusted domain of cloud. To do so, a method may be followed as below:

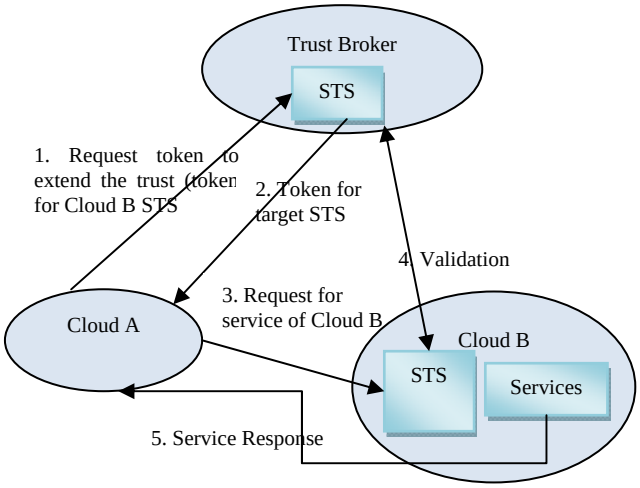

Fig. 1

Whenever a user demands for the service to the Cloud A, that service would be offered to the user. If the service is not available within the Cloud A, then Cloud A will extend the domain of trust internally without interrupting the user by following some secure steps as in Fig. 1.

In the step 1, Cloud A send the authentication request to the STS/ trust broker. Cloud A presents its credential (previously, issued by Trust Broker) to the STS. Then, STS validates the credentials and it may also decide whether to issue a security token for the authenticated cloud A. In step 2, authentication token may be issued if the cloud's credential is validated successfully. After getting the authentication token, In the step 3, cloud A sends a service request message that includes the issued security token from STS. In step 4, The STS of the Cloud B validates the security token by communicating the STS which issued the token. Cloud B STS determines whether it is issued by trusted STS and the token was not tempered. In the step 5, the service initializes and sends a response message to the client. In this way, a secure channel between Cloud A and Cloud B is formed with the STS actions and the service may be offered to the interested user through Cloud A (internally collaborating with Cloud B) successfully.

V. Conclusion

Services offered by the extension of trusted domain of cloud may resolve the issues of security lack, unavailability of services, restriction of the cloud and incompatibility. In this way, a composite trustworthy cloud process is formed which allow users to access a single point of Iaas, Paas and Saas services easily and securely.

References

[1] Sameer Rajan and Apurva Jairath, "Cloud Computing: The Fifth Generation of Computing", Proceedings of the IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2011, India
[2] Urjita Thakar, Vandan Tewari, Sameer Rajan," A Higher Accuracy Classifier based on Semi-supervised Learning", IEEE International Conference on Computational Intelligence and Communication Networks (CICN), 2010, India.
[3] Bernd Mohr, Computational Nanoscience: Do It Yourself!, John von Neumann Institute for Computing, Julich, Vol.31, pp. 491-505, 2006.
[4] Distributed Computing: Utilities, Grids & Clouds, ITU-T Technology Watch Report 9, 2009.
[5] Wu, Z. and Weaver, A. C. (2007), "Requirements of federated trust management for service-oriented architectures" International Journal of Information Security**,** Vol. 6(5), pp. 287 – 296.
[6] Z. Wu and A. C. Weaver (2005), "Dynamic trust establishment with privacy protection for web services", Proceedings of the IEEE International Conference on Web Services(ICWS'05)
[7] Z. Wu and A. C. Weaver (2006), "A privacy preserving enhanced trust building mechanism for web services", Deptt. of computer science, University of Virginia
[8] Z. Wu and A. C. Weaver (2007), "Using web services to exchange security tokens for federated trust management", IEEE International Conference on Web Services (ICWS 2007).

Authors Profile

Sameer Rajan has completed his *Bachelor of Technology* degree in Computer Science and Engineering from **Northern India Engineering College**, Lucknow, Uttar Pradesh (India) and *Master of Engineering* degree in Computer Engineering from **Shri Govindram Seksaria Institute of Technology and Science (SGSITS)**, Indore, Madhya Pradesh (India). Presently, he is working as Scientific Officer and he is also The District Informatics Officer (DIO) in ***National Informatics Centre (NIC)***, *Department of IT, Ministry of Communications and Information Technology, Government of India (GoI).* His research areas of interest are Cloud Computing, E-Governance and Data Mining.

Apurva Jairath has completed her *Bachelor of Engineering* degree in Information Technology from **Guru Ramdas Khalsa Institute of Science and Technology (GRKIST)**, Jabalpur, Madhya Pradesh (India) and also *Master of Engineering* degree in Computer Engineering from **Shri Govindram Seksaria Institute of Technology and Science (SGSITS)**, Indore, Madhya Pradesh (India**).** Presently, she is working as Assistant Professor in the department of Computer Science and Engineering in ***Gyan Ganga Institute of Technology and Sciences (GGITS)***, *Jabalpur, Madhya Pradesh (India).* Her research areas of interest are Cloud Computing and Wireless Technology.