Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2014, Vol. 6, No. 4

Multi-Agent based Framework for Secure and Reliable Communication among Open Clouds

Amjad Mehmood

Institute of Information Technology, KUST, Kohat, KPK, Pakistan

Tel:+92-922-520282 E-mail:.amjad.mehmood@kust.edu.pk

Houbing Song

Department of Electrical and Computer Engineering, West Virginia University, USA

Tel: + 304-442-3076 E-mail:.h.song@ieee.org

Jaime Lloret

Instituto de Investigación para la Gestión Integrada de Zonas Costeras (IGIC), Universidad Politecnica de Valencia, Spain

Tel: +34-609549043 E-mail: jlloret@dcom.upv.es

Received: July 24, 2014 Accepted: November 9, 2014 Published: December 27, 2014

DOI: 10.5296/npa.v6i4.6028 URL: http://dx.doi.org/10.5296/npa.v6i4.6028

Abstract

Cloud Computing (CC) is an emerging field of Information Technology. CC environment completely relies on the perception of utility, service-oriented, cluster and grid computing. The idea of virtualization discriminates CC from other fields. CC environment provides better, reliable, and scalable services. Since clouds are working independently smooth, but standalone, cloud operation is complex. Therefore the need of interoperability and portability with other clouds come into play which increases the scope of the cloud environment. Then, the security threats are increased in the cloud environments. In order to address the problem, a Secure Multi-Agent based framework for Communication among Open Clouds is proposed in this paper. In the framework, each cloud has a secure Mobile Agent which is responsible of the secure communication among clouds. Thus, authentication of Mobile Agents is performed by the Directory Agent. Directory agents are included in order to avoid the joining malicious or attacker mobile agents into the cloud. The theoretical and practical results show that Multi-agent based framework is more reliable and secure than other cloud environments.

Keywords: Cloud Computing, Distributed Computing, Security Authentications, Mobile Agents, Interoperability, Portability, Communication, Reliability.

1. Introduction

Cloud Computing (CC) has done great achievements in the field of Information Technology by providing better and cheaper services over the internet to on demand and rent basis customers [1-4]. CC major achievement progresses with the maturity of different technology in the field of computer science. It provides high-quality software, scalable infrastructure, utility software, and platform to their customers. There are several CC providers who are proving services to their users on demand basis [5]. There are different types of clouds with regard to their services to the users, e.g.

- PRIVATE CLOUDS
  - Venture hold or rent
- COMMUNITY CLOUDS
  - Cloud that is made for some specific group of people or community.
- PUBLIC CLOUDS
  - Cloud for all types of people
- HYBRID CLOUDS
  - Combination of different clouds leads to hybrid cloud.

Moreover, each cloud normally offers different types of services to their users, which can be classified as:

- SaaS: Software as a Service. Cloud provides Software to their users.
- PaaS: Platform as a Service. It offers Platform to the users for developing their soft-wares.
- IaaS: Infrastructure as a Service. It provides infrastructure to their users.

CC is being used in a wide range of fields such as vehicular communications [6][7], wireless ad hoc and sensor networks [8][9] and multimedia networks [10].

Almost all the companies that use CC services provide security for interoperability and portability. On the other hand, many attackers are trying to breach the security to take over cloud resources [11].

Security means the data or information couldn't be accessed by an unauthorized way for the purpose for use, disclosure, interruption, change, read through copying etc. information or data contain four things regarding security. In fact, these are the principles of security.

1. **Confidentiality**: This principle helps to take-care about the contents to keep protected from the malicious user. It's also defined as Privacy of information. The disturbance of the privacy of data or information is defined as an interruption. It can further be explained as looking into the data without interrupting it.
2. **Integrity:** In this technique such a change in data or system which affects the functionality of the real work and data exactness is negotiated. So data are modified by unauthorized users. Now the breaking of integrity is defined as a modification. So if the integrity is compromised so data will be inconsistent as well.
3. **Availability:** In the principle, it is ensured that data or information remains available to all the users properly. The challenge for availability is the interruption.

4. **Authentication:** This is the process to verify that whether the user is valid or otherwise. There are a number of ways for the authenticity of the user to prove that he/she is valid or not, but the most important is that the user has a username and password for authenticity.

Security is one of the main concerns of CC environment which could increase users of the clouds. Similarly, security at the interoperability level is also very important and vital as well. Because, if the cloud is secure, but to whom it wants to communicate is not secure, then ultimately it is not secure as well. There are many research communities who are working to address the problems related to interoperability. The interoperability needs come into play when the serving cloud has not enough resources or lack of services, or user wants to change its cloud provider, or shutdown/busy due some technical problems, or clouds want to work jointly etc.

In the paper authors have proposed a security mechanism for CC using multi-agent system architecture. It is proved that using such architecture CC's interoperability and portability issues can be made secure than the existing one.

The rest of the paper has arranged as follows. The related work is presented in Section 2, the proposed work is given in Section 3, the Network Security is defined in Section 4, and Section 5 describes the Experiments and Evaluation of existing and proposed work. Finally, Section 7 presents the conclusion and future work of the paper.

2. Related Work:

Intercloud communication is becoming one of the major challenges nowadays [12]. Many researchers have addressed the problem of portability and interoperability among the open clouds, and trying to propose solutions [13]. A. Singh et al. proposed an intelligent framework for communication between clouds via agents [14]. The paper provides an excellent framework for an agent, for bringing scalability in clouds, and provides an efficient algorithm for better and easy communication. In the framework each cloud registers it's that agent with the Directory Agent (DA), the DA gives acknowledgement to the cloud after its registration for future correspondence. Once agents of the clouds get registered with the DA, they start communication and interaction with each other. As there is no security mechanism involved in checking the authenticity, integrity, availability, and confidentiality of the malicious agents. Therefore, malicious agent could register itself with the DA, and hence they compromise the security of all the registered agents.

A. Mehmood et al. proposed an authentication & authorization approach, for authenticated services in Multi-Agent System, in which public key infrastructure (PKI) & operating system concept of sand box is used for direct & indirect security concern respectively [15, 16].

Z. Zhang et al. also worked on cloud interoperability and portability by combining the advantages of both Mobile agent and CC, to bring the realization of open cloud federation [17]. R. Rajagopal et al. present the model for security during the process of interoperability to the CC environments and grid computing [18]. M. Kretzschmar et al. focused their research in [19] on CC environment security as well as interoperability challenges and issues.

K. Ren et al. discussed in [20] that security is the main concern for its extensive embracing of CC based environments. This paper further proposed the security mechanism by addressing different security challenges for public cloud environments.

3. Proposed Framework

The basic purpose of this framework is to provide secure interoperability, portability, and the communication among the different clouds among cloud computing environments. In order to increase the scope of clouds in-term of processing, infrastructure, application, utility and other services, it needs to communicate with other clouds. So as standalone cloud existence is not possible in the world of commutation, similarly, security comes first, and considered the most important element to motivate the communication.

Therefore, keeping in mind the same we intend to propose the simple approach called Multi based Framework for Secure and Reliable Communication among Open Clouds. All the MAs are registered with directory services, therefore, MAs of the cloud got the information about each other registered in the directory. This is one of the advantages of a Directory Agent, which it is not only helping MA to interact with each other, but also provides them security which makes it different from the traditional cloud framework.

3.1 System Overview

Since each cloud has its own standard, therefore, interoperability and portability among the clouds are not possible. Intended to which, the concept of Foundation for Intelligent Physical Agents (FIPA) based agents is introduced, because agents are interoperable by default [21]. Hence, coordination and communication among the open clouds [13] is possible through an agent. An Agent is defined as software which acts independently and exhibits autonomously without constantly being told [21]. Consequently, using the same concept, Mobile Agent (MA) is introduced, which represents a cloud [14]. In the framework, MA is the mandatory or soul element of the clouds. Each MA, has a unique name to identify it globally. Moreover, MA registers itself with the DA. So when the cloud requires interoperability or portability features, it comes to DA, where it suggests the cloud which cloud's MA is the best for the cloud. The selection of best cloud depends upon, the user feedback, and successfully services offered to the clients in a smaller amount of time. After a recommendation, it sends the acknowledgement to the cloud. So cloud requesting cloud's MA starts communication with the recommended cloud's MA.

The basic theme of the paper is, that during the communication and coordination, security, which is one of the most important issues, and unfortunately, fewer efforts have been done, to address the problem [14]. Once the problem gets solved, then it could attract more users to the services offered by the clouds. Consequently, it increases the usage of services providing by the clouds. Similarly, as our framework also offers the best cloud to the user, so each cloud would have to increase QoS. Our proposed framework is more secure and intelligent due to MAS architecture, and, moreover, all the clouds are administered easily as they are registered at one directory. So, it maintains the security of the framework easily.

Now when the request cloud's MA comes, it checks DA, whether it is a valid cloud (valid clouds list has already been provided to the DA), if DA finds it valid, it performs an authentication process, and finally registers it to DA, otherwise DA regrets it. Hence, the framework avoids the malicious registration of the MA. MA is mobile code based systems, which enhancing the features of software agents such as autonomy, reactivity, proactively, communication and social ability, by providing them mobility [22].

Now, when the cloud is acknowledged, it gets the registration ID. It can start the communication and coordination with the recommended cloud's MA. By using the same key MA of the cloud signs into the DA. The DA finds out whether the MA is valid or not. If it finds out valid, then DA assigns the best MA to the cloud to perform the operation of interoperability, and portability. This process avoids the registration and submission of malicious or intruder cloud's MA to the DA. Consequently, more reliable and authentic communication takes place among the clouds.

In case DA has more than one best clouds. It sends a list of clouds to requested cloud. Then the cloud selects the best cloud as per his demands. But in the most cases, it performs automatically by the communicating clouds on the basis of MA's intelligence, which it perceives from the behavior of the cloud.

After the communication has taken place, the requesting cloud fills out the Performa including the following parameters of Table 1.

Parameter Name	Value	Parameter Name	Value
Service Completion Status	Completed Successfully, an unsuccessful (Shows reliability of the service)	**Time of Allocation**	Start time of the transaction
Finish Time	Finish time of the transaction	**Cost**	Depend upon size of data received and bandwidth allocated
Location	Name of the cloud nominated by the framework	**Date**	Date of the transaction
Receive data	Data Received in MBs	**Data rate**	Bandwidth
Services Requested	Name of the Services required by the cloud	**Services Provided**	Name of the services provided
Size	Size of the data	**Remarks**	Final remarks of the cloud bout the cloud assigned by DA

Table 1: Parameters of the Performa Filled by Requesting Cloud after Communication

The Performa is submitted to DA and DA selects the best cloud's MA. So when any request comes, DA rightly mentions the best MA. Table 1 not only helps the user in selecting the best cloud, but also removes the MA's of cloud from the list, if it does not improve its value for the specified period of time.

Since all clouds register their MAs at the DA. Therefore, we could perform some kind of planning at DA. As each cloud does know the status and information of other clouds, which helps the coordination and communication among the open clouds. Moreover, the DA also forms a list like Table 2 (after evaluating the MA's of the cloud plus the feedback form).

Parameter Name	Value	Parameter Name	Value
Cloud Name	Shows Cloud Name	**Services offered**	List services it offered
Infrastructure Name	Infrastructure details	**Utility Services available**	List services it offered
Vender Name	Show Vender Name	**Cost**	Depends upon speed they provide and Time they consume
Platforms available	List the name of platforms deals with	**History**	List of work done by the cloud
Type of Cloud	What type of cloud? (On the basis of the past history and feedback submitted by the user decide the best cloud)	Remarks	Some Remarks

Table 2: List of Parameter of the individual cloud at DA

Unlike traditional cloud security (where security is applied to each cloud separately), in our framework, secure is provided at DA's level. After this security policy, the secure communication has been increased.

3.2. Steps for Cloud's Mobile Agent Authentication

1. DA is the place where all the MA's of the clouds are registered and provides the public key to the MA of the cloud and keeps the private key to himself.
2. When a service requested by user is not available at local cloud then MA of that particular cloud comes into play.
3. Once MA gets activated, it uses the public key to request the DA.
4. The DA gets its public key and performs authentication process if successful, it provides the best MA to the requesting MA but if a tie exists among more clouds then list is provided to the MA, otherwise regrets the request.
5. In case of list MA takes a decision of selecting the best cloud on the basis of parameters provided to the MA of the clouds e.g. better and cheaper in rates etc.
6. Once the decision has been taken, MA starts communication and interaction with the MA of recipient cloud.
7. After communication users submit a feedback form to the DA about his satisfaction regarding the communication, then local MA combines its and user's comments and submit it to DA, it records the feedback in its database for future evaluation of the MAs.
8. On the basis of feedback i.e. as parameters defined in Table 2, Hence, DA makes the life of the MA competitive.
9. On receiving positive feedback to any cloud, then rating and priority goes higher, therefore, in future more users are prompted to select that particular cloud for their services.
10. Otherwise, the rating goes down, and then MA is warned by the DA, to improve its behavior otherwise, its priority goes so down that no MA will select them in the future.

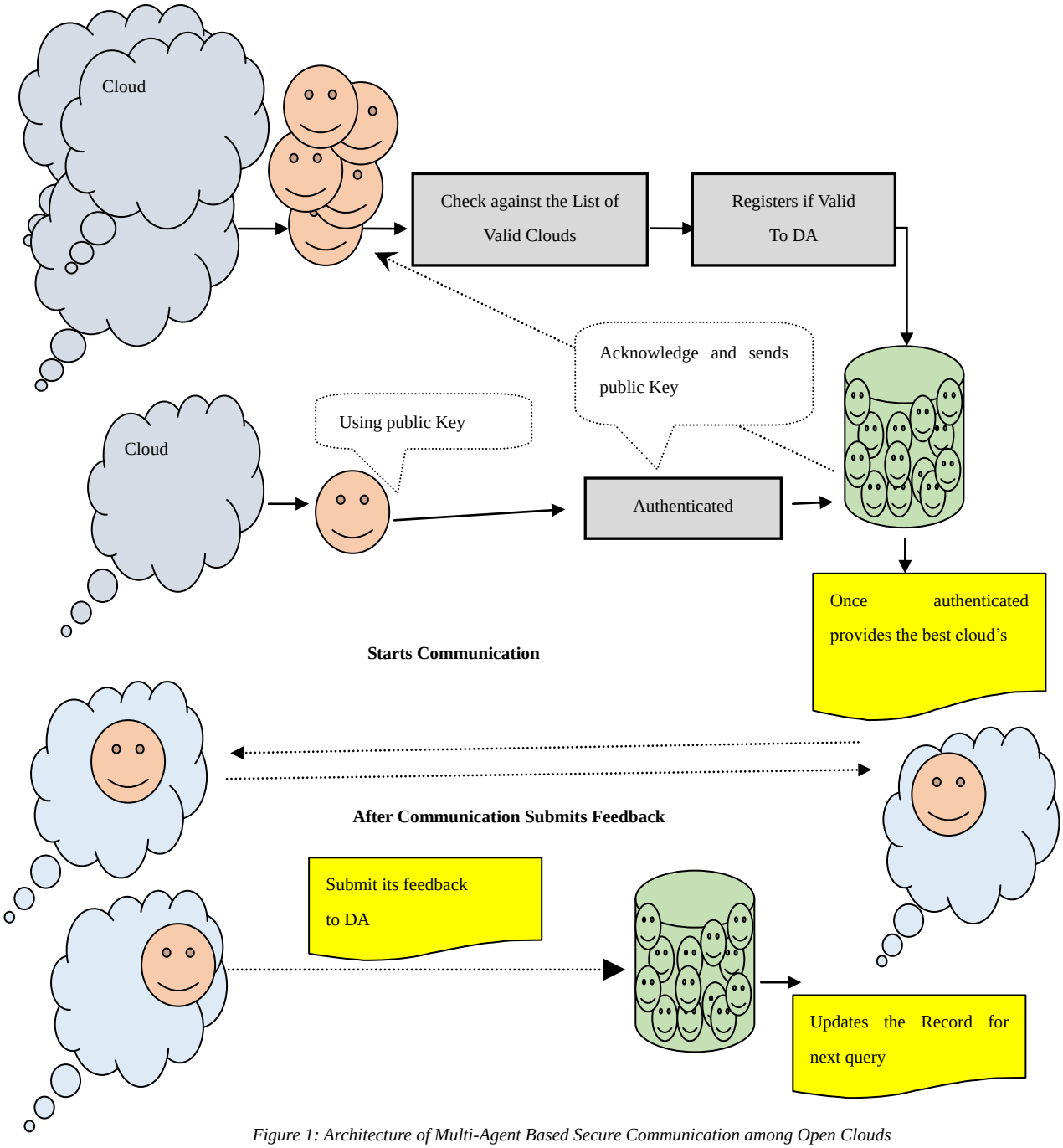

Figure 1: Architecture of Multi-Agent Based Secure Communication among Open Clouds

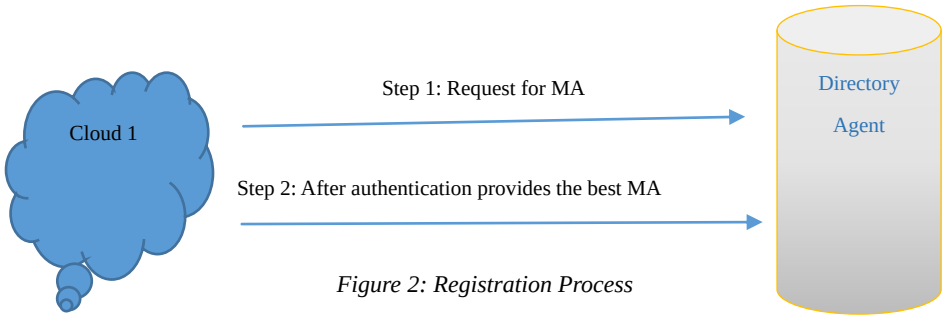

Figure 2: Registration Process

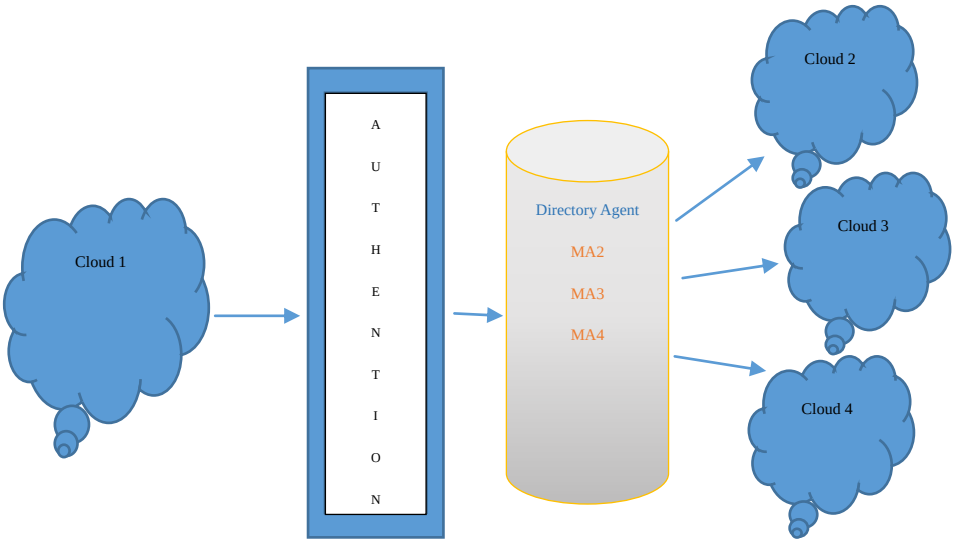

Figure 3: Authentication process of the cloud

Figure 2 shows the registration process of, that's it how MA of the clouds are registered with the directory agent. Cloud sends registration request to the directory agent. Figure 3 shows the authentication process is performed to check the cloud, if the cloud is already registered or not. If the cloud is valid then directory agent sends an acknowledgement to the cloud that it has been registered, and using the same identity MA could access the directory agent for its service requirements.

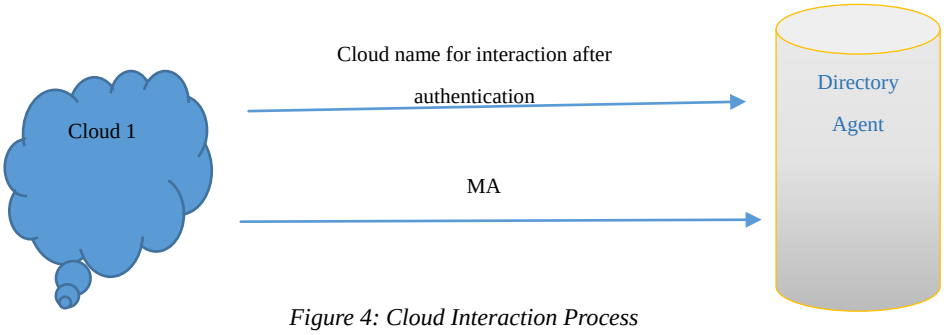

Figure 4: Cloud Interaction Process

Figure 4 demonstrates that when cloud requests services from some other clouds for interaction or communication. Then first it requests to directory agent, so after authentication, it allocates requested the cloud's mobile agent to particular cloud's mobile agent.

For authentication purpose, we use the same technique that has been used in SECURING SERVICES IN MULTI-AGENT SYSTEMS. This research paper gives a very novel mechanism of checking the validity of the MA. In this technique MA is registered to DA just as an agent registers to Agent Directory Services in Multi-agent System architecture. Once it gets registered in the directory, it receives a registration ID from the DA. Table 1, shows the parameters that how DA finds that it's valid cloud. When it finds valid, it gets registered by the DA, and assigns it a unique registration ID, which helps DA to get authenticated the MA, by the time of request for the services see Figure5.

Algorithm for Registration

- Start

  Reg = Registration;

  Ack = Acknowledgement;

  C = Content;

  K = Key;
- Interoperability needed by the cloud, Activates MA Then
- MA Comes to DA
  - If valid (See Table. 1) Cloud
  - Registered
    - IF cloud == registered Then
      - C = true
      - K =true
    - Else
      - C = False
      - K=False
      - Sends an acknowledgement
      - Contains Public Key for future access
      - DA keeps private key
  - Else
    - Access Denied

3.3. Steps for Authentication of Cloud:

A MA registers itself with the DA to avail the services. When MA wants to interact with any other cloud's MA, it enters into DA, which receives both key and contents from the MA. Then it applies the formula to get the registration ID from the MA, which it had assigned to MA at the time of registration. If registration ID matches with the one stored in DA, then it would be authenticated, otherwise it regrets the service requested by the MA. Following are the steps which are taken during cloud authentication:

1. The MA provides content and key that has been given after the MA registration.
2. The DA takes the content and key.
3. The Key ((CK_e+H_{cke})+header) is divided by CK_e and H_{cke}
4. The CK_e (CK_E given by the agent) is checked with the CK_e stored in DA.
5. IF the agent CK_e is match with DA Then
   1. Admission is taken.
6. If does not match with DA then
   1. Dined admittance.

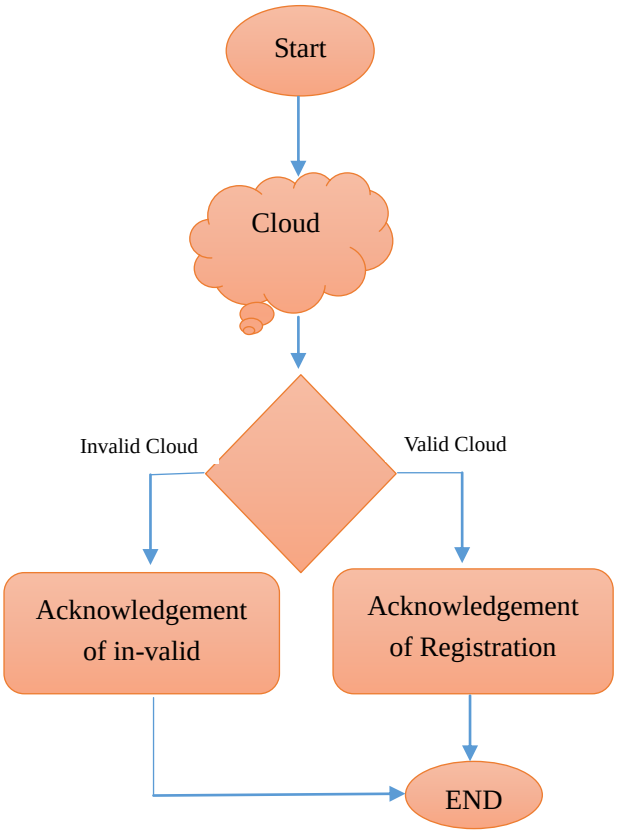

Figure 5: Steps for Authentication of Clouds

Parameters	Directory Agent	Tradition Clouds
Security	Most secure because in this framework all the clouds register their Mobile Agent (MA) with directory agent, so the user needs the authentication before get the permission to access the cloud.	Security is dependent upon the cloud providers, so cloud would be secure if each cloud provider provides the security mechanism to its cloud services.
Interoperability	As a cloud's MA are located in directory agent therefore, each mobile agent has done homework before, and planned to settle with other MAs for interoperability.	Traditional clouds have no homework or planned before, for interoperability in case of open clouds i.e. it performs this business when it is active.
Portability	Same as above	Same as above
In-convince	Less In-convince	Most chances of In-convince
User's Satisfaction	Intelligent to take care of the user	Not intelligent to take care of the user
Performance	Use all the resources of directory are at the single pool, therefore, utilization of resources is high.	Each cloud's utilization is different and it might be possible that resource utilization is low.
Cost	Less cost, because all MAs are registered at one place, therefore, all clouds need not to deploy for each provider.	The cost is high.
Quality of Cloud	Take care of the quality and user comments on the clouds, which help clouds to improve.	No such mechanism.

Table 3: Comparison between our proposed framework and Tradition Cloud framework

It is observed that proposed framework can enhance the cloud's against different parameters especially security. So we draw comparisons between the two as per following Table 3.

4. Network Security

Measurements regarding network security are desired to guard data during transmission flanked by terminal client and computer and between computer to computer [15] [16]. And presently, no protocols are available to provide security for the cloud so that it safely communicates with each other.

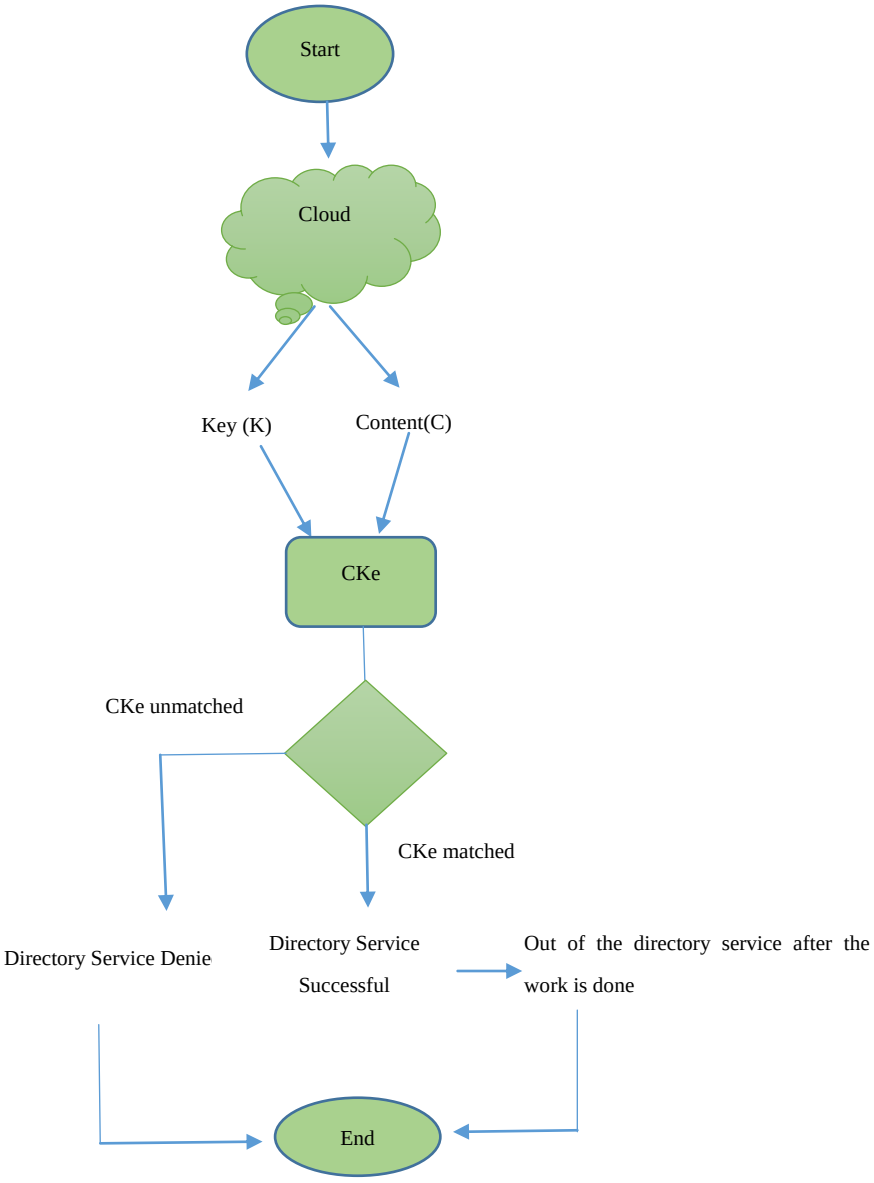

Figure 6: Flow chart for Authentication

The figure 6 shows the overall architecture of the proposed solution, i.e. to develop secure and reliable communication using Multi-Agent based frame. By using this architecture, it is evaluated that the secure communication among the open clouds are considered to be more reliable than its competitor protocols.

5. Experiments and Evaluation

In this section, we perform some experiments using CloudSim [23] in order to simulate a CC environment. The experiments have been conducted on a Celeron machine having the hardware feature shown in table 4.

Operating System	Ubuntu Linux Version 8.04,
Process	1.86GHz with 1MB of L2 cache
RAM	1 GB
Software	JDK 1.6.

Table 4: System requirements for cloudsim

In order to evaluate the overhead in housing a simulated CC environment that consists of a single data center, with four clouds with following features: vender based cloud (Azure), Agent based cloud, open cloud, and FIPA directory based cloud (proposed), considering those environments number of experiments have been performed. For the experiment 5 users are registered with each cloud. We have performed about 400 experiments on each and got the results on average to get the best on the attributed mentioned in figures. As the goal of these tests was to calculate the reliability, interoperability, portability, incontinence, user-satisfaction, Security, and computing power requirement to instantiate the Cloud simulation infrastructure, no attention has given to the user workload.

For the memory test, we profile the total physical memory used by the hosting computer in order to fully instantiate and load the CloudSim environment. The total delay in instantiating the simulation environment is the time difference between the following events: (i) the time at which the runtime environment (Java virtual machine) is directed to load the CloudSim program; and (ii) the instance at which CloudSim's entities and components are fully initialized and are ready to process events.

Figures 7 and 8 present, respectively, the amount of time and the amount of memory is required to instantiate the experiment when the number of hosts in a data center increases. The growth in memory consumption (see Fig. 8) is linear, with an experiment with 100000 machines demanding 75MB of RAM. It makes our simulation suitable to run even on simple desktop computers with moderated processing power because CloudSim memory requirements, even for larger simulated environments can easily be provided by such computers.

5.1 Testing

In this section our proposed framework based on FIPA architecture's performance is challenged, while we are comparing it with the performance of a framework uses a client/server approach. For testing purpose, the mathematical model used which was created and applied by Peter Braun in 2004 [24]. Our aim is to verify our framework functionality and effectiveness. The framework with the Mobile Agent approach claims the less network load compare to the client/server approach, by shipping code to data instead of shipping data to code [25]. Fig. 7 compares the network loads of doing intrusion by client server case, and Mobile Agent approach. As a result the framework with Mobile Agents will produce a lower network load when the number of clients to visit is less than six hosts. It means that the framework Control Center should not add more than six clients to the itinerary of the Mobile Agents to make the Mobile Agent's task efficient and optimized. However, the issue of migration strategies has not been considered in the equation. Accordingly, less code and data will be relocated. And therefore even less network load will be produced by our approach.

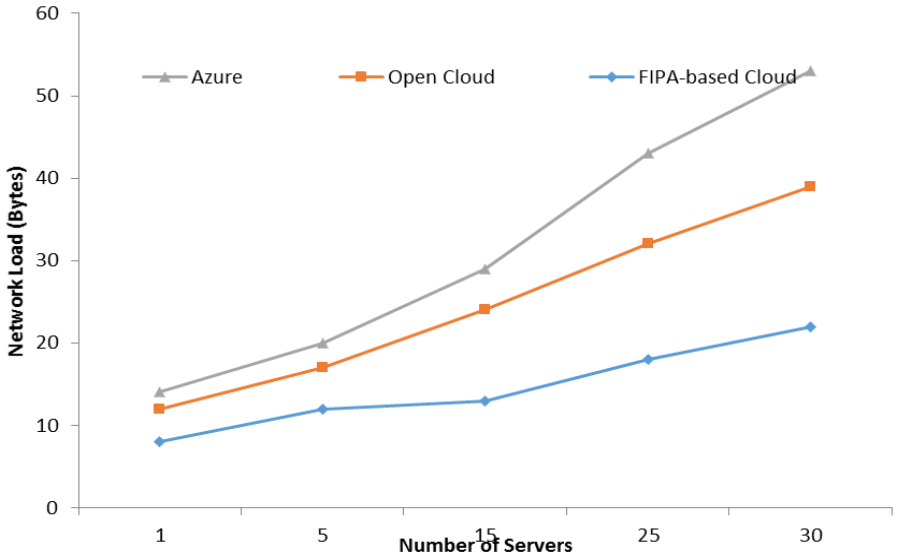

Figure 7: FIPA based Cloud Comparison with others

In the figure 8, we have demonstrated the response time of both the open cloud and FIPA based Azure cloud architecture. Hence it shows that the FIPA based cloud shows less response time as compared to openccloud.

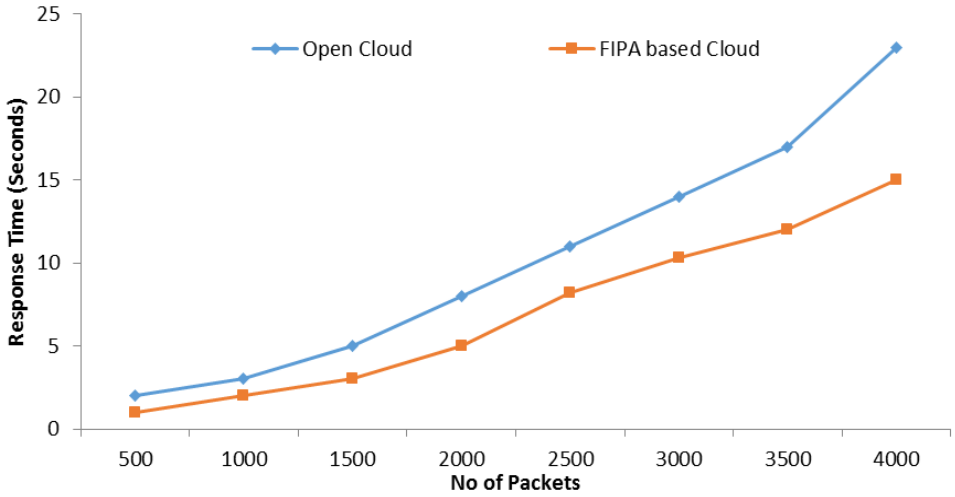

Figure 8: FIPA based and Open based Cloud Comparison

In the figure 9, Denial of Service (DOS) Attack has been demonstrated and proved that FIPA based clouds are more reliable and robust or scalable than the Open cloud based systems.

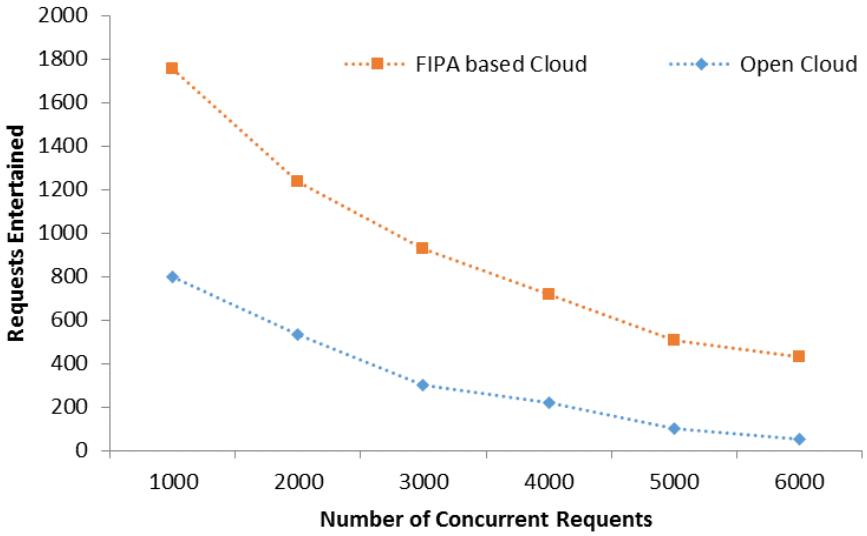

Figure 9: DOS based Comparison between FIPA and Open based Cloud

6. Comparison of three Cloud Environment

Figure 10 Shows the comparison drawn among three clouds based environments e.g. Azure, Open Cloud and FIPA based. It demonstrates that the FIPA based cloud environment outperforms the closed source, and Open source CC environment. In the experiment, we considered the parameters like reliability, interoperability, portability, incontinence, user satisfaction, and the most important one of them is security.

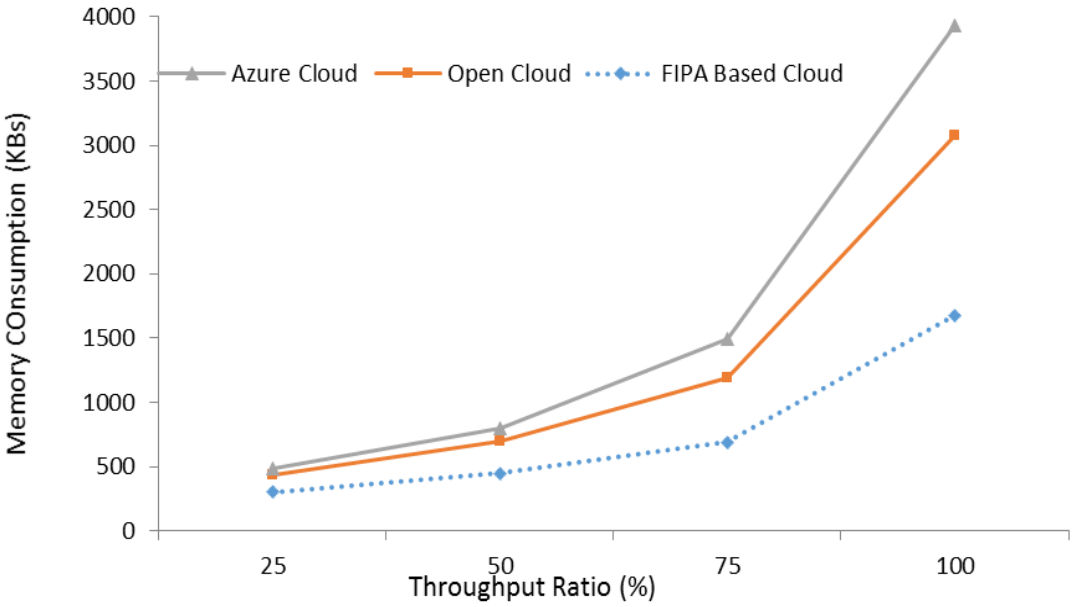

Figure 10: Comparison of the three CC Environments

6. Conclusion and Future Work

Our proposed work provides secure communication among the open clouds using Multi-Agents System based architecture. It further provides security to the DA. In order to avoid the interference of malicious or an intruder attacked to the DA. The experimental results show that Multi-Agent based framework is more secure as compared to the other CC environment. Moreover, Quality of Services (QoS) is also improved by using the framework. In future we will work to develop an adaptive transport protocol, which would help the framework to adapt with the environment during any communication with the other non FIPA based CC environment accordingly.

References

[1] K. Ren, C. Wang, Q. Wang, (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73. http://dx.doi.org/10.1109/MIC.2012.14

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, M. Zaharia, (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58. http://dx.doi.org/10.1145/1721654.1721672

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599-616. http://dx.doi.org/10.1016/j.future.2008.12.001

[4] M. Amjad, (2013). An Agent Tilting Solution For Communication Among Open Clouds, published by LAMBERT, Academic Publishing, Germany.

[5] N. M. Chowdhury, R. Boutaba, (2010). A survey of network virtualization. Computer Networks, 54(5), 862-876. http://dx.doi.org/10.1016/j.comnet.2009.10.017

[6] Kayhan Zrar Ghafoor, Kamalrulnizam Abu Bakar, Marwan Aziz Mohammed, Jaime Lloret (2013), Vehicular Cloud Computing: Trends and Challenges, Mobile Networks and Cloud computing Convergence for Progressive Services and Applications, IGI Global, Pp. 262-274. http://dx.doi.org/10.4018/978-1-4666-4781-7.ch014

[7] Jiafu Wan, Daqiang Zhang, Shengjie Zhao, Laurence T. Yang and Jaime Lloret (2014), Context-Aware Vehicular Cyber-Physical Systems with Cloud Support: Architecture, Challenges and Solutions, IEEE Communications Magazine, Vol. 52, Issue 8, Pp. 106-113. http://dx.doi.org/10.1109/MCOM.2014.6871677

[8] Raquel Lacuesta, Jaime Lloret, Sandra Sendra, and Lourdes Peñalver (2014), Spontaneous Ad Hoc Mobile Cloud Computing Network, Vol. 2014, Article ID 232419, 19 pages. http://dx.doi.org/10.1155/2014/232419

[9] Lucas D. P. Mendes, Joel J. P. C. Rodrigues, Jaime Lloret, and Sandra Sendra, Cross-layer Dynamic Admission Control for Cloud-based Multimedia Sensor Networks, IEEE Systems Journal, Vol. 8, Issue 1, Pp. 235 - 246. February 2014. http://dx.doi.org/10.1109/JSYST.2013.2260653

[10] Joel J. P. C. Rodrigues, Liang Zhou, Lucas D. P. Mendes, Kai Lin, and Jaime Lloret, Distributed Media-Aware Flow Scheduling in Cloud Computing Environment, Computer Communications, Vol. 35, Issue 15. Pp. 1819-1827. September 2012. http://dx.doi.org/10.1016/j.comcom.2012.03.004

[11] Hero Modares, Jaime Lloret, Amirhossein Moravejosharieh, Rosli Salleh, (2013) Security in Mobile Cloud Computing, chapter of the book Mobile Networks and Cloud computing Convergence for Progressive Services and Applications, IGI Global. Pp. 79-91, http://dx.doi.org/10.4018/978-1-4666-4781-7.ch005

[12] Jaime Lloret, Miguel Garcia, Jesus Tomas, Joel J. P. C. Rodrigues (February 2014), Architecture and Protocol for InterCloud Communication, Information Sciences, Vol. 258. Pp. 434-451. http://dx.doi.org/10.1016/j.ins.2013.05.003

[13] Spring, 2009, OpenCloud (2009) "The Open Could Manifesto" dedicated to the belief that the cloud should be open. Available at http://www.cyclopaedia.info/wiki/Open-Cloud-Manifesto

[14] P. S. Hada, R. Singh, M. M. Meghwal, (2011). "Security Agents: A Mobile Agent based Trust Model for Cloud Computing" International Journal of Computer Applications 36(12):12-15, December 2011.

[15] I. Zeeshan, M. Amjad, H. Muhammad, G. Abdul (2008). "Securing Services in Multi-Agent Systems" 1st National Conference on Security, Computing, & Communication (1st NC-SCC 2008), KUST, NWFP, Pakistan pp. 20-21, May 23-25, 2008, KUST, Kohat, NWFP, Pakistan.

[16] Z. Iqbal, A. Mehmood, A. Ghafoor, H.F. Ahmed, A. Shibli, (2007, November). Authenticated service interaction protocol for Multi-Agent System. International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET 2007). 18-20 November 2007. Dubai, EAU. http://dx.doi.org/10.1109/HONET.2007.4600276

[17] Z. Zhang, X. Zhang, (2009, November). Realization of open cloud computing federation based on mobile agent. IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS 2009). 20-22 November 2009. Shanghai, China. pp. 642-646). http://dx.doi.org/10.1109/ICICISYS.2009.5358085

[18] R. Rajagopal, M. Chitra, (2012, July). Trust based interoperability security protocol for grid and Cloud computing. IEEE Third International Conference on Computing Communication & Networking Technologies (ICCCNT 2012), July 26–28, 2012. SNS College of Engineering, Coimbatore, Tamilnadu, India. http://dx.doi.org/10.1109/ICCCNT.2012.6396030

[19] M. Kretzschmar, S. Hanigk, (2010, October). Security management interoperability challenges for collaborative clouds. 4th IEEE International DMTF Academic Alliance Workshop on Systems and Virtualization Management (SVM 2010). 25-29 October 2010 Ontario (Canada). Pp. 43-49. http://dx.doi.org/10.1109/SVM.2010.5674744

[20] K. Ren, C. Wang, Q. Wang, (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73. http://dx.doi.org/10.1109/MIC.2012.14

[21] P A. Mehmood, A. Ghafoor, H.F. Ahmed, Z. Iqbal, (2008). Adaptive Transport Protocols in Multi Agent System, Fifth International Conference on Information Technology: New Generations (ITNG 2008), Las Vegas, NV, April 7-9, 2008. http://dx.doi.org/10.1109/ITNG.2008.57

[22] Sophos Security Threat Report 2013. Available at http://www.sophos.com/en-us/medialibrary/pdfs/other/sophossecuritythreatreport2013.pdf

[23] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, César A. F. De Rose, and Rajkumar Buyya (2011), CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms, Software – Practice and Experience, 41:23–50, http://dx.doi.org/10.1002/spe.995

[24] Braun, W. R. Rossak (2005). Mobile agents: Basic concepts, mobility models, and the tracy toolkit. Amsterdam. Elsevier.

[25] R. Khan, A. Mehmood (2013). Realization of Interoperability and Portability among Open Clouds by using Agent's Mobility and Intelligence. International Journal of Advanced Computer Science, 3(11). Pp. 544-549

Copyright Disclaimer