Privacy in Cloud System

Tariq Alwada'n
Computer Science Department
The World Islamic
Sciences and Education
University
Amman, Jordan

Adel Hamdan Mohammad
Computer Science Department
The World Islamic
Sciences and Education
University
Amman, Jordan

Hamza Aldabbas
Prince Abdullah bin
Ghazi Faculty of
Information and Technology
Al-Balqa' Applied University
Salt, Jordan

ABSTRACT
Cloud computing technology is used as inexpensive systems to gather and utilize computational capability. This technology improves applications services by arranging machines and distributed resources in a single huge computational entity. Clouds consist of data centers which are owned by the same institute. The homogeneity within each data centre in the infrastructure is the main feature for the cloud computing but any conflict between heterogeneous data centers and/or different administration domains can become a serious issue for cloud interoperability and privacy. This paper suggests a new framework to solve the interoperability problem.

General Terms
Distributed Systems, Computer Resources.

Keywords
Cloud, Policy Management, Grid Services, Security, Privacy.

1. INTRODUCTION
Cloud computing is a huge amount of distributed and dynamic resources from storage, computing power and services that are provided on request to customers over the Internet [16]. In general, the cloud computing resources locates in a huge data storage centre and is organized by a third party, who offers computing infrastructures which can be accessed from anywhere by anyone with internet services [9]. Many authors, such as [6, 13, 18, 10, 17], sketch out the fact that cloud computing is a modern distributed computing environment and business concept, that supplies software, computing power and storage on demand, distributed over the internet. The main words in the prior description are (on demand). The use of cloud computing is variety from handling and managing large scale of data, resolving complex scientific challenges utilizing clouds and organizing login to medical records for example [12]. Figure (1) shows the architecture model for the cloud computing.

Such an example of a cloud computing is Amazon's Elastic Compute Cloud (EC2) [1] which allows clients to "rent" computer slots in Amazon's data centre. Generally, this feature is used in coordination with another data storage service called Amazon's Simple Storage Service (S3) [2]. The cost of these services either to be calculated in relation to the disk storage that being used by the customer's monthly and extra costs for data transfer, or charged in relation of instance-hours; one instance-hour can be defined as the data handling ability for a specific computational element for one hour [9].

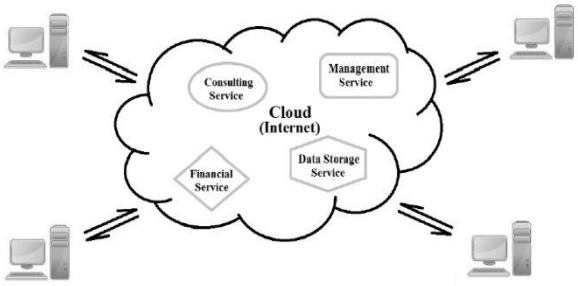

Fig. 1. Cloud Computing [14, 3]

Another example of utilizing cloud computing is what Rolim et al.[20] has introduced to utilize cloud computing in the Health Care Institutions. Where "sensors" are connected to medical tools and equipments which are then inter-connected to swap services with other institution's computing network services and installations by utilizing computing and wireless sensor networks. Later the data becomes presented in the cloud, and then processed by professional teams or distributed to medical parties for examination. This system is considered a low cost way to enhance the quality of medical support delivery [24].

Generally the two main methods that can be used to utilize the cloud computing environment are; in one method the cloud cluster holds the user's application, which can be presented as a web service reachable to any person with an internet connection. As examples of this type of services are Gmail, YouTube and Google Maps. In the second method the user sends a huge scale of data to the cloud cluster along with the needed application codes for processing this data. Later, the cloud clusters process these data using the user's application and return the results back to the user. It can be seen that in both methods the user's applications and data locate (for some time) on the cloud environment, which is managed and organized by a third party, which may create a really big problem related to the privacy and policy issues [9].

Many people may confuse between the cloud technology and grid technology. A grid is a system that has the ability to manage and organize resources and services that are distributed across several control domains, utilize protocols and interfaces and supply high quality of service [8]. Grimshaw et.al. [11] defines grid computing as "coordinated resource sharing and problem solving in dynamic, multi-institution virtual organizations". The homogeneity within each data centre in the infrastructure is the main feature for the cloud computing compared to grid computing. But any conflict between a heterogeneous data centre and/or different

administration domains can become a serious issue for cloud interoperability and privacy. Cloud interoperability is generally about the ability of being able to work with other platforms and other applications not only in one environment but in most of cloud environments. On the other side, grids were originally established with the knowledge that resources infrastructure are dynamic and heterogeneous in their nature. This implies different organization with different administrative domains. This also means that security and privacy were taken into account from the beginning when the grid system was originally built.

The infrastructure of the cloud normally depends on web models (over SSL) to establish and access account information for the external users, and allows them to change or reset their keys (passwords) with a new ones by email in what can be considered as unencrypted communication [16]. This means the privacy of the users' data and ability to give the permissions to handle this data to a specific domains or users by the original data owner is less than expected. On the other hand, the situation in the grid environment is completely different, where the grid administrators or grid users can control the handling of their data or the permission and policies over their resources. Presently, the security paradigm for clouds appears to be less secure than the model in grids environment. Security is an essential element in cloud computing. For any Cloud environment, there should be methods to offer security, including authentication, authorisation and data encryption. It can be seen that the stages of anonymity and privacy provided by cloud to the external users will be less than the user of desktop in numerous situations [7].

Our proposed framework introduces a solution that may solve the privacy issue by giving the policy of the users the control over their data. Policies are groups of regulations, standards and practices written by one or more owners of jobs or administrators of resources about how their resources, jobs or data can be handled and used. Policies decide how a job should be done, how security is applied in a domain and how an organization organizes, secures and distributes their resources. The rest of the paper is organized as follows: The next section presents related works to cloud systems. Section three describes a new cloud model called Cloud Computing Deployment Models. The fourth section introduces our new framework while the fifth section describes the component of our cloud policy architecture and describes each component in details. In the last section we discuss future possibilities and conclude the paper.

2. RELATEDWORKS

Buyya et al.[4] describes cloud computing and presents the architecture for generating market oriented clouds by utilizing methods like Virtual Machines (VMs). Xiao et al.[25] uses web pages to small screen devices. This method depends on making use of the huge storage and computing resource of cloud computing to create a new wireless web access method. Vieira et al.[22] presents a way to detect intrusion in cloud and grid environment in which checking data is gathered from the cloud. In this solution every node detects local incidents that have the ability to present security abuses and be aware of the reset of the nodes. Each single Intrusion Detection System (IDS) together with other (IDS) contributes in intrusion detection. The system collects data from different sources, like the service, log system and node messages. The (IDS) service examines this data and employs detection methods based on user knowledge and behavior of earlier attacks. If it senses an intrusion, it employs the middleware's communication methods to transmit alerts to the rest of the nodes. According to that, the (IDS) service improves the security level in the cloud by using two intrusion detection techniques. The behavior based method; which is used to evaluate current user actions to the normal behavior. The second method is the knowledge based method; which is used to identify known footprints belonging to the attacks or specific series of actions from a user which could symbolize an attack.

3. CLOUD COMPUTING DEPLOYMENT MODELS

This is a new model concept that can be divided into the following four famous models (but there might be other models that can be drawn from them) [5]:

—Public: Services and resources are reachable to the public by using the internet. This environment emphasises the advantages of rationalization (as a user has the ability to utilize only the needed services and pay only for their use), operational simplicity (as the system is organized and hosted by a third party) and scalability. The main concern in this type of cloud environment is the security; since this environment is accessible to the public and user data in one stage is hosted by a third party.

—Private: Services and resources are reachable within a private institute. This environment emphasises the advantages of integration, optimization of hardware deals and scalability. The main concern is the complexity, as this environment is organized and hosted by internal resources. Security is not a main issue compared to the public cloud as the services are reachable only through private and internal networks.

—Community: Services and resources of this type are shared by various institutes with a common aim. It may be organized by one of the institutes or a third party [19].

—Hybrid: This type combines the methods from the private and public clouds. Where resources can be used either in a public or a private cloud environment [21]. The advantages and the concerns are a mixture of the earlier type.

Another cloud technology which has become very popular recently is called Green Cloud Computing. It's aim is to reduce resource consumption and yet fulfil quality of service needed and hold the resources switched off as long as possible. "The advantages of such technology are lower heat production and power saving by employing server consolidation and virtualization technologies; since active resources (servers, network elements, and A/C units) that are idle lead to energy waste" [24, 23].

4. CLOUD POLICY: NEW FRAMEWORK

Before the users can submit their data or run their applications on a certain source or system they may need to guarantee that this source or system has not been compromised which could result in their own application or data being stolen or which could result in asking for certain users to be allowed to access the service [15]. That means the user policy should be taken into account when taking the final decision. This paper is proposed a policy-managed cloud environment that addresses the user-submitted policy. Traditional authorization policy management frameworks act well in authorization policy for a single cloud environment that belongs to one administrator, where the contributing hosts grant the permission to follow a global authorization system. However most of policy management tools do not provide a clear support for sharing

resources between multiple cloud environments. Therefore; the question is:

How to present a policy framework that can support the user policy and enforcing data policies in its designs to support multiple cloud environments?

This paper is proposed a framework that provides the features of supporting the external User Policy (UP) along with enforcing policies for data movements within the cloud environment. Our framework simply depends on sending the user's policy along with the user data and/or application(s). Figure (2) shows this process. Before the owners send their data or applications, they choose the user and/or the organizations that allow their data to be sent to them. Also the owners can choose to which country their data allowed to be stored or manipulated. This policy that been sent along with the owners' data or application is traveled along with the data or application all the time. That means this policy should be applied all the time.

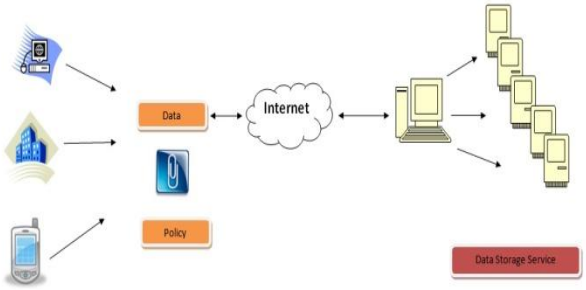

Fig. 2. Sending the Policy with the user data

5. ARCHITECTURE COMPONENTS

Our framework consists of two agents: Cloud Policy Agent (CPA) and Policy Management Agent (PMA). Figure (3) shows our agents. The (CPA) is the main agent in the cloud which arranges and contacts the policy agents for each organization. (PMA) is the Policy Agent that represents each organization.

After the authorized cloud users submit their data or applications to the cloud environment the cloud system sends the users' polices to the (CPA) which by its turn asks the Policy Management Agent (PMA) if the users' policies allows its data or applications to be stored or manipulated in its servers, and if the (PMA) allow this specific user to manipulate their data on their servers. If all the policies passed throw the agents, in this case the data that been sent to cloud system can be stored or manipulated safely.

At this point the privacy of the user's data and applications have been guaranteed, and at the same time prevented some intruded users or organizations from making use of cloud system. This feature is another advantage of our framework. As it is not only gives the external user the ability to control their own data but also give the cloud system administrators the ability to choose their costumers and also creating black lists for some users, and that lists can be shared and exchanged between different cloud administrators to create some kind of earlier security step.

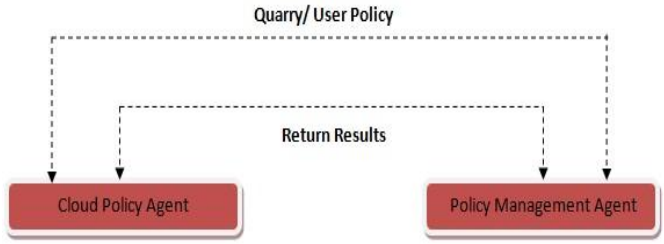

Fig.3. Framework Agents

6. CONCLUSIONS AND FUTURE WORK

Cloud computing technology is used as inexpensive systems to gather and utilize computational capability. Clouds consist of data centers which are owned by the same institute. But any conflict between heterogeneous data centers and/or different administration domains can become a serious issue for cloud interoperability and privacy. This paper suggests a new framework to solve the interoperability and privacy problem. In this paper a new dynamic policy management framework was presented, this framework has the capability to deal with policies of multiple cloud systems which organized by different administrators and at the same time has the feature of enforcing users' policies for data and application within the cloud. Based on our contributions, we are confident that our framework for policy organizing may solve the privacy problem in cloud systems. Our future work is concerned with conducting more experiments on our framework to see the effect of the policies on the cloud systems.

7. REFERENCES

[1] Amazon. Amazon elastic compute cloud (amazon ec2), 2012.

[2] Amazon. Amazon simple storage service (amazon s3), 2012.

[3] M.-E. BEGIN. An egee comparative study: Grids and clouds- evolution or revolution. EGEE III, project Report, 30, 2008.

[4] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications, HPCC '08, pages 5–13, Washington, DC, USA, 2008. IEEE Computer Society.

[5] Shirlei Aparecida de Chaves, Rafael Brundo Uriarte, and Carlos Becker Westphall. Toward an architecture for monitoring private clouds. IEEE Communications Magazine, 49(12):130–137, 2011.

[6] Shirlei Aparecida de Chaves, Carlos Becker Westphall, and Flavio Rodrigo Lamin. Sla perspective in security management for cloud computing. In Proceedings of the 2010 Sixth International Conference on Networking and Services, ICNS '10, pages 212–217, Washington, DC, USA, 2010. IEEE Computer Society.

[7] KEVIN J. DELANEY and VAUHINI VARA. Google plans service to store users' data, NOVEMBER 27, 2007.

[8] I. Foster and K. Kesselman. The grid: Blueprint for a future computing infrastructure. In Morgan Kaufmann in Computer Architecture and Design, 1999.

[9] Ian Foster, Yong Zhao, Ioan Raicu, and Shiyong Lu. Cloud computing and grid computing 360-degree compared. 2008 Grid Computing Environments Workshop, abs/0901.0(5):1– 10, 2008.

[10] Ian Foster, Yong Zhao, Ioan Raicu, and Shiyong Lu. Cloud computing and grid computing 360-degree compared. 2008 Grid Computing Environments Workshop, abs/0901.0(5):1– 10, 2008.

[11] A. S. Grimshaw, M. A. Humphrey, and A. Natrajan. A philosophical and technical comparison of legion and globus. IBM J. Res. Dev., 48:233–254, March 2004.

[12] Eric Hand. Head in the clouds, 24 October 200.

[13] Thomas Heyman, Riccardo Scandariato, Christophe Huygens, and Wouter Joosen. Using security patterns to combine security metrics. In Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, pages 1156–1163, Washington, DC, USA, 2008. IEEE Computer Society.

[14] Fei Hu, Meikang Qiu, Jiayin Li, Travis Grant, Draw Tylor, Seth McCaleb, Lee Butler, and Richard Hamner. A review on cloud computing: Design challenges in architecture and security. CIT, 19(1):25–55, 2011.

[15] Marty Humphrey and Mary R. Thompson. Security implications of typical grid computing usage scenarios. Cluster Computing, 5:257–264, July 2002.

[16] Paul Jaeger, Jimmy Lin, and Justin Grimes. Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology Politics, 5(3):269–283, 2008.

[17] Neal Leavitt. Is cloud computing really ready for prime time? Computer, 42:15–20, January 2009.

[18] Lijun Mei, W. K. Chan, and T. H. Tse. A tale of clouds: Paradigm comparisons and some thoughts on research issues. In Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference, pages 464–469, Washington, DC, USA, 2008. IEEE Computer Society.

[19] Peter Mell and Timothy Grance. The nist definition of cloud computing (draft) recommendations of the national institute of standards and technology. Nist Special Publication, 145(6):7, 2011.

[20] Carlos Oberdan Rolim, Fernando Luiz Koch, Carlos Becker Westphall, Jorge Werner, Armando Fracalossi, and Giovanni Schmitt Salvador. A cloud computing solution for patient's data collection in health care institutions. In Proceedings of the 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine, ETELEMED '10, pages 95–99, Washington, DC, USA, 2010.IEEE Computer Society.

[21] Borja Sotomayor, Rub´en S. Montero, Ignacio M. Llorente, and Ian Foster. Virtual infrastructure management in private and hybrid clouds. IEEE Internet Computing, 13:14–22, September 2009.

[22] K Vieira, A Schulter, C B Westphall, and C M Westphall. Intrusion detection for grid and cloud computing. It Professional, 12(4):38–43, 2010.

[23] J. Werner, G. Geronimo, C. Westphall, F. Koch, and R. Freitas. Simulator improvements to validate the green cloud computing approach. In Network Operations and Management Symposium (LANOMS), 2011 7th Latin American, pages 1 –8, Oct. 2011.

[24] C. M; KOCH F. L.; ROLIM C. O; VIEIRA K. M.; R. S.; BRINHOSA R. B.; GERONIMO G. A.; FREITAS R. R. WESTPHALL, C. B; WESTPHALL. Management and security for grid, cloud and cognitive networks. Revista de Sistemas de Informao da FSMA, 8:8–21, 2011.

[25] Yunpeng Xiao, Yang Tao, and Qian Li. A new wireless web access mode based on cloud computing. In Proceedings of the 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application - Volume 01, PACIIA '08, pages 645–649, Washington, DC, USA, 2008. IEEE Computer Society.

.