ISSN 2278-5612

Trust Models in Cloud Computing - A Perspective

Shyamlal Kumawat[1], Prof. Deepak Tomar[2]
Department of Computer Science , Technocrats Institute of Technology Bhopal, India
shyam.kumawat31@gmail.com
Department of Computer Science , Technocrats Institute of Technology Bhopal, India
tomar_deepak01@yahoo.in

ABSTRACT

Cloud computing is a new paradigm in which dynamically scalable virtualized computing resources, services and information are provided as a service among the people and organizations across the globe over the Internet. The recent developments in cloud computing technology placed numerous challenges in the field of Cloud Computing, including data replication, consistency, reliability, availability and scalability of cloud resources, portability, trust, security, and privacy. Still most of the organizations are not adapting cloud computing due to lack of trust on service provider. This paper gives an overview of cloud computing, and discusses trust and related security challenges. The important elements of cloud environment, which shapes the users trust and provides a way of evaluating each element's importance, are emphasized. Although there are many technological approaches that can develop trust in cloud provider and improve cloud security, there are currently no one-size-fits-all solutions, and future work has to tackle challenges such as trust model for security, as well as suitable mechanisms for ensuring accountability in the cloud. As trust based schemes have been widely discussed and applied in a lot of cloud computing scenarios, becoming subject of scientific researches, this paper also presents a survey of few trust models.

Indexing terms/Keywords

Cloud Computing, Cloud Security, Trust, Trust Models, SaaS, PaaS, IaaS..

Academic Discipline And Sub-Disciplines

Science; Technology;

SUBJECT CLASSIFICATION

Informaion Technology

TYPE (METHOD/APPROACH)

Survey

Council for Innovative Research
Peer Review Research Publishing System
Journal: International Journal of Management & Information Technology
Vol. 6, No. 2
editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 2278-5612

1. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Cloud has been increasingly adopted in many areas, such as banking, e-commerce, retail industry, and academy [18]. In recent years, industries such as Amazon, Microsoft, HP, Google and IBM have heavily invested on Cloud infrastructure and underlying technologies. Citrix and VMware provided core technology of virtualization in Cloud computing. This shows that there is a growing trend of using cloud platforms for ever rising storage and data processing needs.

The highly distributed and non-transparent nature of cloud computing represents a considerable obstacle to the acceptance and market success of cloud services [16].Our study supports that in the context of data security and trust which is a major element and is either missing or not efficient in the currently existing computing models. Despite the fact that service providers use various mechanisms to ensure high level of data security, potential users of these services often feel that they lose control over their data and they are not sure whether cloud providers can be trusted. Since users do not have direct control over their files on cloud provider's datacenter, the trust evaluation would be a critical issue for them [3]. That is why we strongly support a trust management mechanism between the cloud service provider and users. Our work contributes to the understanding of why trust establishment is important in the Cloud computing scenario, how trust can act as a facilitator to overcome the barriers and what are the exact requirements for the trust and reputation models (or systems) in Cloud environments to support the consumers in establishing trust on Cloud providers.

The remainder of this paper is structured as follows: Section II introduces the different types of Cloud Computing models also known as Service and Deployment models together with its security implications, Section III explains information security requirements that are applied to Cloud computing followed by Section IV that discusses Cloud computing trust models and finally, we conclude the paper in Section V.

2. CLOUD COMPUTING MODELS

2.1 Types of clouds

Cloud computing model has three service delivery and deployment models [5]. The deployment models are as follows:

a) Private cloud

A Private cloud is solely deployed, owned or rented by an organization. The entire cloud resources are dedicated to that organization for its private use.

b) Community cloud

A Community cloud is similar to a private cloud, but where the cloud resource is shared among members of a specific or closed community that has shared concerns like security requirements, policies etc.

c) Public cloud

A Public cloud is owned by a service provider and its resources are sold to the public. The cloud infrastructure is made available end-users on rent and can typically scale their resource consumption up (or down) to their requirements. Amazon, Google, Rackspace, Salesforce, and Microsoft are examples of public cloud providers.

d) Hybrid cloud

A Hybrid cloud is the combination of two or more cloud infrastructures; these can be private, public, or community clouds.

2.2 Cloud Service Delivery models

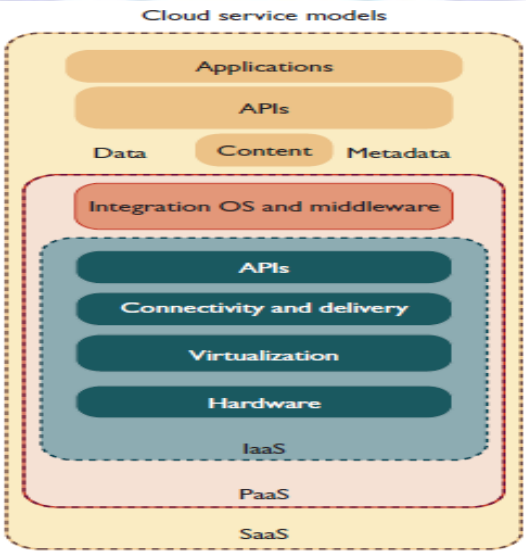

Fig. 1. Cloud Service models

a) Software as a Service (SaaS)

Cloud SaaS is the use of applications running (like online word processing tools and web content delivery services) on a cloud infrastructure to provide services to end-users. SaaS provider hosts the applications and makes the applications available over the network to multiple customers. SaaS can deliver business applications such as customer relationship management (CRM), enterprise resource planning (ERP). Companies that offer SaaS services include Google Apps [12] and Salesforce.com [13]. The consumer does not control underlying infrastructure.

b) Platforms as a Service (PaaS)

Cloud offers a platform to the end-users to run their applications for development environment. The applications are developed and/or acquired by end-users on top of the tools provided. Best examples of cloud PaaS are Microsoft Windows Azure [15] and Google App Engine [12]. The consumer does not control the underlying infrastructure or operating systems, but does control deployment of individual applications.

c) Infrastructure as a Service (IaaS).

Cloud IaaS offers fundamental offers abstracted hardware, operating system as well as virtual machines over the network to provide services to end users. By renting IaaS service, the customers can use the latest extended infrastructure and they do not have to concern with updating the technology. An example of IaaS is Amazon EC2 [14].

2.3 Cloud Computing Concerns

Gartner has conducted an exploration regarding the information security issues that should be considered when dealing with Cloud computing. The following list contains seven security issues highlighted by Gartner [10]. These are leading issues that build trust of end user in cloud provider.

Privileged user access —inquire about whom has specialized access to data, and about the hiring and management of such privileged administrators.
Regulatory compliance— Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Make sure that the vendor is willing to undergo external audits and/or security certifications.
Data location— whether provider will commit to storing and processing data in specific jurisdictions, and whether they will make a contract to obey local privacy requirements on behalf of their customers.
Data segregation—Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
Recovery—Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
Investigative support—Does the vendor have the ability to investigate any inappropriate or illegal activity?
Long-term viability—what will happen to data if the company goes out of business? How will data be returned, and in what format

3. SECURITY REQUIREMENTS IN CLOUD

The security framework of cloud computing platform should guarantee the confidentiality, integrity, non repudiation, availability and reliability of the data in the platform [6]. Each of the security requirements will be highlighted below in context of Cloud computing.

Identification & authentication

In Cloud computing, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly, depending on the type of cloud as well as the delivery model. The individual cloud users are verified and validated by employing authenticity protections to their cloud profiles.

Authorization

Authorization is an important information security requirement in Cloud computing to enforce referential integrity. The referential integrity is exerting control and privileges over process flows within Cloud computing. The system administrator maintains Authorization in a Private cloud.

Confidentiality

In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data located across multiple distributed databases across datacenters. It is a must when utilizing a Public cloud due to its accessibility nature. This characteristic concerns with shielding the sensitive information from the unauthorized disclosure

Integrity

This attribute concerns with accuracy, completeness and validity of information in regard with business requirement policies and expectations. The integrity requirement employs in applying the ACID (atomicity, consistency, isolation and durability) within the cloud domain mainly when accessing data. The ACID properties should be robustly imposed across all Cloud computing deliver models.

Non-repudiation

This attribute concerns with the ability to prevent users from declining the responsibility of the actions performed. Non-repudiation in Cloud computing can be attained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received) [11].

Availability

This feature concerns with information being operational and available whenever it is required by the business process. Availability is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models in Cloud computing.

4. TRUST AND TRUST MODELS

TRUST

The concepts of trust, trust models and trust management has been the purpose of several recent research projects. Trust between service providers and users are extremely necessary for providing better cloud security. For this both the Service providers and the clients must undertake their responsibilities to ensure safety and security of cloud and data on clouds. Most of the organizations are not moving to cloud computing due to lack of trust on service provider. For users to distinct between clouds providers in terms of offered security and trust, there should be some mechanism to evaluate trust services by independent third parties [3]. In a nutshell the purpose of this study is to provide baselines for better trust on cloud service provider.

A survey of existing mechanisms for establishing trust, and comment on their limitations are presented in [16, 17]. Also more rigorous mechanisms based on evidence, attribute certification, and validation based on those limitations are proposed. The paper is concluded by suggesting a framework for integrating various trust mechanisms together to explore trust issues in the cloud. The essential properties and corresponding research challenges to integrate the QoS parameters into trust and reputation systems are identified in [16].

In [2] author proposed a trust calculation process and trust model to ensure a reliable files exchange among nodes, in a private cloud, in accordance with the established metrics. The trust value of a node indicates its suitability to perform the operations between nodes or hosts of cloud. This value is calculated based on the history interactions/queries between the nodes. These values are ranging between [0, 1]. The trustworthiness evaluation is based node storage space, operating system, link and processing capacity. The simulations are done using CloudSim framework to show the efficiency of the model in selecting more reliable node in private cloud.

In [4] authors have proposed a Trust Model between users and cloud providers. In proposed work trust can be established in three turns and when cloud users are satisfied at first two turns then at third turn they can rely on cloud provider. User must be satisfied with previous experience of cloud provider in first turn, at second turn user must have knowledge about SLAs (Service Level Agreements), along with issues related to securities at different levels. Trust is established that cloud provider can be a reliable provider with the satisfaction of implementation of different securities at second turn. User or Organization can trust on reliable cloud provider at third turn.

In [7] Zhidong et al. presented a scheme for building a trustworthy cloud computing environment by integrating a Trusted Computing Platform (TCP) to the cloud computing system. The TCP is used to provide authentication, confidentiality and integrity [5, 6]. This scheme displayed positive results for authentication, rule-based access and data protection in the cloud computing environment.

Zhimin et al. [8] propose a collaborative trust model for firewalls in cloud computing and it is compatible with the firewall and does not break its local control policies. This model uses different security policies for different domains. It considers the transaction contexts, historic data of entities and their influence in the dynamic measurement of the trust value. Trust is measured by a trust value on the entity's context and historical behavior, and is not fixed. The cloud is divided in a number of autonomous domains and the trust relations among the nodes are divided in intra and inter domain trust relations. The intra-domain trust relations are based on transactions operated inside the domain.

In [9] IaaS providers to offer a closed box execution environment that guarantees confidential execution of guest virtual machines (VMs), a trusted cloud computing platform (TCCP) is proposed. Before requesting the service to launch a VM, this system allows a customer to verify whether its computation will run securely or not. The TCCP guarantees the confidentiality and the integrity [5, 6] of a VM user, whether or not the IaaS enforces these properties.

In [6], the "Trust as a Service" (TaaS) framework to improve ways on trust management in cloud environments, is proposed. In particular, an adaptive credibility model is developed that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks. . In addition, TMS allows trust feedback assessment and storage to be managed in a distributed way. The approaches have been validated by the prototype system and experimental results.

5. CONCLUSION

Cloud computing is altering the way industries and enterprises do their businesses. With wider cloud adoption, access to business-critical data and analytics will not just help enterprises stay in front, it will also be critical to their existence. In such a scenario trust between service providers and users is indispensible for providing better cloud security. For this both the Service providers and the clients must take on their responsibilities to ensure safety and security of cloud and data on clouds. In this study different security and trust related research papers were studied briefly. This paper illustrates cloud concepts and explored the security problems in the cloud system. Encouraged by the need to better understand the user's trust in cloud computing services, one presented a survey on few trust models also. In short, the purpose of this study is to provide a broad overview on cloud computing, and specifically how it relates to consumers in terms of security and trust

ACKNOWLEDGMENTS

Authors are cordially giving thanks to the researchers of different trust models, security models of cloud computing and to all those who have tried hard to make cloud simulation tools to make research works easy to accomplish.

REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing, National Institute of Standards and Technology", ver. 15, 9 July 2010.

[2] Edna Dias Canedo, Rafael Timóteo de Sousa Junior, Robson de Oliveira Albuquerque and FábioLúcio Lopes deMendonça, "File Exchange in a Private Cloud supported by a Trust Model", 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 978-0-7695-4810-4/12, IEEE Computer Society 2012.

[3] Ahmad Rashidi and NaserMovahhedinia, "A Model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.2, April 2012.

[4] Shakeel Ahmad, Bashir Ahmad, Sheikh Muhammad Saqib and Rashid Muhammad Khattak, "Trust Model: Cloud's Provider and Cloud's User", International Journal of Advanced Science and Technology Vol. 44, July, 2012.

[5] AkhilBehl, KanikaBehl, "An Analysis of Cloud Computing Security Issues", 2012 World Congress on Information and Communication Technologies IEEE 2012.

[6] Xue Kai, Liu Zhao, Yang Shuguo, Research on Secure Frame of Cloud Computing, Computer & Telecommunication, 2010.

[7] ZhidongShen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[8] Zhimin Y., Lixiang Q., Chang L.,Chi Y., and Guangming W,"A collaborative trust model of firewall-through based on Cloud Computing," Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design. Shanghai, China. pp. 329-334, 14-16. 2010.

[9] N. Santos, K. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing," Proc. HotCloud. June 2009.

[10] Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', *Infoworld*, viewed 13 March 2009, from http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing- security-risks-853?page=0,1

[11] Google, Google Apps. <http://www.google.com/apps/>.

[12] Salesforce. Salesforce CRM applications and software solutions. <http://www.salesforce.com/eu/crm/products.jsp>.

[13] Amazon. Amazon Elastic Compute Cloud (EC2). http://aws.amazon.com/ec2/.

[14] Microsoft. Microsoft Windows Azure. <http://www.microsoft.com/windowsazure/>.

[15] Sheikh MahbubHabib, SaschaHauke, Sebastian Ries and Max M¨ uhlh¨auser, "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing: Advances, Systems and Applications, Springer 2012. http://www.journalofcloudcomputing.com/content/1/1/19.

[16] Jingwei Huang and David M Nicol, "Trust mechanisms for cloud computing", Journal of Cloud Computing: Advances, Systems and Applications, Springer Open Journal 2013, http://www.journalofcloudcomputing.com/content/2/1/9.

[17] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Gener. Comput. Syst. 25 (6) (2009) 599–616, Elsevier Science, Amsterdam, The Netherlands.