View on Security, Privacy and Trust Issues in Cloud Computing Environment

J.K. Verma
School of Computer & Systems Sciences
Jawaharlal Nehru University, New Delhi, Delhi, India

C.P. Katti
School of Computer & Systems Sciences
Jawaharlal Nehru University, New Delhi, Delhi, India

Abstract- Cloud computing is not a new concept. It was envisioned very long back by John McCarthy as delivering computing services similar to the public utilities like water and electricity on metered basis. Cloud computing leverage the power of virtualization technologies which enables the deployment of dynamic workload and allows scale-in and scale-out of its capabilities through rapid provisioning and de-provisioning of virtual machines in an elastic manner. It paves the way to increase capacity or add capabilities dynamically in the existing system without investing in infrastructure. Cloud computing brings about not only convenience and efficiency but also the significant challenges of data security, privacy, and trust issue that make cloud customers reluctant towards its adoption. This paper presents a study on security, privacy and trust issues that are very much prevalent in cloud computing environment.

Keywords – Information Technology, Business, Cloud Computing, Security, Privacy, and Trust.

I. INTRODUCTION

Cloud computing is the long-held dream of information technology world that was envisioned by John McCarthy in 1961 to deliver “computing as a public utility” [1]. It is a hot topic currently in the field information technology industry, academia, government, international agencies and other sectors. Cloud computing is based on large-scale distributed computing paradigm driven by resource pooling of dynamically scalable, highly available, abstracted, virtualized, configurable and reconfigurable computing resources. These resources can be rapidly provisioned and de-provisioned in an elastic manner and requires minimal management efforts at the site of large-scale data centers and distributed resources. Therefore, the term “Cloud computing” is widely used for applications and services that execute over a distributed network or a large scale data center using virtualized resources. The virtualized resources are accessible through commonly used networking protocols [2].

The virtualized and abstracted resources usually refer as Virtual Machines (VM). VMs are the software implementation of the Instruction Set Architecture (ISA) of computer hardware at the application layer of the system that helps in abstraction of the resources from underlying hardware. Virtualization technologies enable partitioning of hardware resources into multiple isolated VMs that are capable of executing programs like independent computing machine and allow live migration of VMs from one server to another server [3]. However, virtualization leaves room for leakage of data due to the reasons that data stores away from the local machine and data moves from single tenant to the multi-tenant environment [4].

Cloud computing delivers computing services as a utility similar to the public goods on a metered basis that follows "pay-as-you-go" model. Figure 1 shows the schematic representation of cloud computing technology indicating that how the cloud computing framework offers its services ubiquitously to multiple platform digital devices [5].

J.K. Verma et al. outlines several issue related to cloud computing paradigm in [1]. They raised a point that "Cloud computing offers a wide variety of advantages, but many problems also exist in its usage. Current researchers and practitioners say that security and privacy are the main causes of concern for people when they adopt cloud computing.” Therefore, we devote this paper to the study of security, privacy and trust issues in cloud

computing environment which seems to be solemn and grave issues for the progress of this technology. The rest of the paper is organized as follows. Section II presents views on the security issue in cloud computing followed by privacy issue and trust issue in Section III and Section IV respectively. Lastly, Section V concludes the paper.

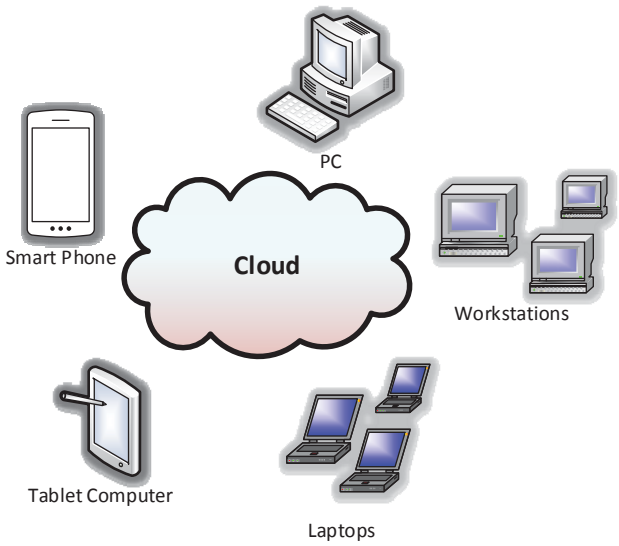

Figure 1: Schematic Representation of Cloud Computing

II. View on Security Risks

Cloud computing poses significant challenges to the field of data security. Data security becomes a bottleneck problem due to two primary reasons: (i) The data stores away from local machine to a distributed computing environment whose nodes are situated in geographically apart locations; and (ii) The data moves from single tenant to multi-tenant environment due to the inherent property of distributed computing environment and involvement of multiple computing nodes. Using a private cloud may be the solution to the problems related to data security because interacting with the outer world is the ultimate need of business for further growth. Therefore, a system can not behave as a closed system, and the system is required to be opened ultimately to achieve new ventures. However, an open system brings about the problem of data leakages due to the reasons aforementioned, therefore, need to be tackled from some other way.

The other possible ways seek the information that are vulnerable to security threats. Z. Tang et al. attempted to identify that what kind of data need to be protected in cloud computing environment and outlined that the following data is considered to be important that need to be protected from outer world [6]:

A. *Personally identifiable information* such as name, ID number, address, social relation information, postal code, Internet protocol, the card number of credit.

B. *Sensitive information* such as religion, race, health, sexual orientation, union membership, or other information like personal finance information, biometric information, job performance information or collection of surveillance camera images in public places.

C. *Usage data* such as input habits, patterns like digital content, product usage history, recently visited websites, frequently visited places or social interaction.

D. *Unique device identities* such as information of uniquely traceable devices like IP address, RFID tags, and unique hardware identities.

Brodkin through light upon the prominent security risks that are pointed out by Gartner in [7]. These points are to important to keep in mind by a potential cloud computing customer and to raise when a customer is going to select a cloud provider:

A. Privileged user access – In cloud computing, services are outsourced actually, and outsourced services bypass the physical, logical and personnel controls over the data deployed in the cloud-like environment. Therefore, Gartner suggests to collect as much as information about the hiring and oversight of privileged administrators, and the control over their access.

B. Regulatory compliance – Cloud service providers are subject to external audits of data hosted on cloud and security certifications. The cloud providers who do not undergo the available scrutiny mechanism gives indications towards their erroneous behavior.

C. Data location – The location of data hosted on clouds is unknown usually. The claim against loss of any data fall under jurisdiction mechanism available in the territory of the country where the data is located. Therefore, it is necessary to ask the provider and commit for storing and processing the data in particular jurisdictions or some contractual commitment for obeying local privacy policy requirements on behalf of the customer.

D. Data segregation – Cloud computing is a shared environment, and host data within it. Encryption of data does not provide complete relaxation towards threats to data security. Therefore, data should be segregated so that others can not encroach upon the data that does not belonging to them. “Encryption accidents makes data totally unusable, and even normal encryption can complicate the availability” [7].

E. Recovery – In case of disaster, a complete loss of data may occur. Therefore, Gartner says that "Any offering that does not replicate the data and application infrastructure across the multiple sites is vulnerable to a total failure." Therefore, a cloud provider should be asked for the ability to complete restoration of data and the time required to complete the process of recovery.

F. Investigative support – In a cloud environment, the data for multiple customers are co-located at times and data is spread across a large number of servers and data center. The data stored on servers changes its location as well as per the need of the underlying system. Therefore, investigating in the cloud environment for any inappropriate or illegal activity is a tough row to hoe.

G. Long-term viability – Business world is very dynamic in nature, and one cloud provider company may be acquired by another larger company due to day to day business dynamics. Therefore, a cloud provider must be asked that how would one can get data back and about data’s particular format so that another cloud can import the data without any modification in such situation.

III. View On Privacy Issue

Cloud computing suffers from privacy and confidentiality concerns because the service provider has access for all the data. This data can be accidentally or deliberately disclosed or used for unauthorized purposes. Privacy is an ability of an individual to closister the information from the world and and revealing it selectively se per the need arises by the individual herself. From an organization’s point of view, privacy means application of available laws, mechanisms, standards, and processes by which personally identifiable information are managed [8]. On the other hand from commercial point of view, consumer context and privacy needs protection and appropriate use of the information about customers and meeting expectations of customers about its use. Privacy issue can be sub-categorized into four following categories [8] [9] [10] [11]:

(i) Users are having control over their data when it is processed and stored in the cloud, avoiding theft, nefarious use, and unauthorized resale of data.

(ii) Guarantying data replication at multiple sites within jurisdictions and in the consistent state, avoiding data loss, leakage, and unauthorized modification or fabrication.

(iii) Ensuring responsible party for the legal requirement for personal information.

(iv) Identifying, checking and ascertaining the extent of involvement of sub-contractors for processing of data.

IV. View On Trust Issue

Trust is the term which is viewed as a measurable belief that utilizes experience of an individual to make trustworthy decisions. The term "Trust" is originally used in social sciences in relation to constructing human beings relationship. "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" [12]. Trust is now an essential substitute for forming security mechanism in distributed computing envronments, as trust as many soft security attributes, such as, reliability, dependability, confindence, honest, belief, trustfulness, security, competence, and suchlike. The trust issue involves following two aspects [8]:

A. *Weak Trust Relationship* – The instance of weak trust relationship occurs due to many reasons. For example, non-delivery of services quickly in the event of non-availability of resources, loss of control in passing sensitive information to the other organizations that are doing cloud transactions, involvement of sub-contractors for delivery of key business processes, non-transitive relation relation trust in customer to cloud provider chain etc. are some identified instance. For enhancement of the capacity of the cloud, new contractors are added to the system in a short period and leaves no room for adequate verification about their identity, practices, reputation and trustworthiness. Additionally, 'on-demand' and 'pay-as-you-go' model further leads to the weak trust realationship.

B. *Lack of customer Trust* – The lack of trust arises in customers due to the instances when personal information is requested by cloud provider and customers are not aware that why the information is asked and how the information will be processed that ultimately leads to the suspicion and distrust [13]. Security related issue are very much prevalent in cloud computing, involvement of personally identifiable information, compliance risks, and non-assurance of addressing such risks by cloud providers make customer reluctant to adoption of cloud computing environment in full-fledged manner.

Trust is very subjective issue in nature as it is uncertain, non-symmetric, context dependent, and partially transitive in nature [14] [15]. Trust issues is sub-categorized into following four categories [10] [11] [16]:

(i). How to define and evaluate the trust according to the unique attributes of cloud computing?

(ii). How to handle the recommended malicious information, which is critical in cloud computing environment, as trust relationship in the cloud is temporary and dynamic?

(iii). How to consider and provide and provide different security level of service according to the trust degree?

(iv). How to manage trust level change with interaction time and context, and to monitor, adjust, and reflect trust relationship dynamic change with time and space?

V. Conclusion

Security threats are the major obstacle for opening up the new era of the long held dreamed vision of visionary and practitioners of information technology world to deliver computing services as a utility in ubiquitous manner. Encryption techniques alone are not sufficient to get rid of the issue and opens room for new problems like encryption accidents that makes data totally unusable and even normal encryption can complicate the availability problem. Privacy and trust issues further deepens the same problem and make potential customers reluctant for adoption of cloud service. This paper study and highlight major security, privacy and trust issues for cloud computing environment in current context and recognize tangible and intangible threats associated with its usage. On the other hand, this paper suggest some remedial options also to the potential cloud customers before selection of cloud provider.

REFERENCES

[1] J. K. Verma and C. P. Katti, "Study of Cloud Computing and its Issues: A Review," *Smart Comput. Rev.*, vol. 4, no. 5, pp. 389–411, Oct. 2014.

[2] J. K. Verma and C. P. Katti, "MADLVF : An Energy Efficient Resource Utilization Approach for Cloud Computing," *I.J. Inf. Technol. Comput. Sci. Inf. Technol. Comput. Sci.*, vol. 06, no. 07, pp. 56–64, Jun. 2014.

[3] J. K. Verma and C. P. Katti, "A Comparative Study into Energy Efficient Techniques for Cloud Computing," in *IEEE Proc. 2nd Int. Conf. on Computing for Sustainable Global Development (INDIACom-2015)*, New Delhi, India, 2015, pp. 2062 – 2067.

[4] C. Almond, "A practical guide to cloud computing security," *A white Pap. from Accent. Microsoft*, 2009.

[5] J. K. Verma and C. P. Katti, "A Survey on Load Balancing Techniques in Cloud Computing Environment," *Int. J. Latest Trends Eng. Technol.*, vol. 5, no. 2, pp. 469 – 478, Mar. 2015.

[6] Z. Tang, X. Wang, L. Jia, X. Zhang, and W. Man, "Study on Data Security of Cloud Computing," in *Spring Congr. on Engineering and Technology (S-CET - 2012)*, Xian, China, 2012, pp. 1–3.

[7] J. Brodkin, "Gartner: Seven cloud-computing security risks," *Infoworld*, Framingham, MA, pp. 1–3, Jul-2008.

[8] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in *IEEE Proc. 2nd Int. Conf. on Cloud Computing Technology and Science (CloudCom - 2010)*, Indianapolis, IN, 2010, pp. 693–702.

[9] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," *Procedia Eng.*, vol. 15, pp. 2852–2856, 2011.

[10] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Gov. Inf. Q.*, vol. 27, no. 3, pp. 245–253, Jul. 2010.

[11] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[12] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Acad. Manag. Rev.*, vol. 23, no. 3, pp. 393–404, Apr. 1998.

[13] A. Tweney and S. Crane, "Trustguide2: An exploration of privacy preferences in an online world," *Expanding the Knowledge Economy: Issues, Applications, Case Studies*. IOS Press, 2007.

[14] S. I. Ahamed, M. M. Haque, M. E. Hoque, F. Rahman, and N. Talukder, "Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments," *J. Syst. Softw.*, vol. 83, no. 2, pp. 253–270, Feb. 2010.

[15] K. Karaoglanoglou and H. Karatza, "Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values," *J. Syst. Softw.*, vol. 84, no. 3, pp. 465–478, Mar. 2011.

[16] A. Sangroya, S. Kumar, J. Dhok, and V. Varma, "Towards analyzing data security risks in cloud computing environments," in *Information Systems, Technology and Management*, Springer, 2010, pp. 255–265.