TECHMIND RESEARCH
ISSN: 2292-1648
International Journal of Management Excellence
Volume 3 No.2 June 2014

An Overview of Public Cloud Security Issues

Atefeh Heydari[1], Mohammad Ali Tavakoli[2], Mohammad Riazi[3]
[1]Faculty of Computer Science and Information System, UTM, Malaysia-81310,
a_tav_ir@yahoo.com
[2]Faculty of Computer Science and Information System, UTM, Malaysia-81310,
m_tav_ir@yahoo.com
[3]Faculty of Computer Science and Information System, UTM, Malaysia-81310,
mohammadriazi@gmail.com

Abstract- *Traditionally, computational needs of organizations were alleviated by purchasing, updating and maintaining required equipments. Beside expensive devices, physical space to hold them, technical staffs to maintain them and many other side costs were essential prerequisites of this matter. Nowadays with the development of cloud computing services, a huge number of peoples and organizations are served in terms of computational needs by large scale computing platforms. Offering enormous amounts of economical compute resources on-demand motivates organizations to outsource their computational needs incrementally. Public cloud computing vendors offer their infrastructure to the customers via the internet. It means that the control of customers' data is not in their hands anymore. Unfortunately various security issues are emerged from this subject. In this paper the security issues of public cloud computing are overviewed. More destructive security issues are highlighted in order to be used by organizations in making better decisions for moving to cloud.*

General Terms- *Security of Public Cloud Computing*

Keywords- *cloud computing; security issues; public cloud; data integrity and confidentiality; cloud security; privacy; moving to cloud; security models*

1. INTRODUCTION

Competition, benefit, reducing costs, increasing incomes and generally staying alive in business environment is the foremost essential target for any organization. Majority of Today's organizations and enterprises are severely depended to computational processes. Investing for not only purchasing servers, computers and other tools but also maintaining them is very costly. Besides installing, using and maintaining these equipments needs IT employees and expertise knowledge. Therefore most of the companies tend to outsource their computational needs to public cloud computing services. For instance, various enterprises such as insurance companies, data banks and hospitals need very large memory to store their data and archive it. Cloud service providers consequently offer large store capacities which are suitable for them, so computing resources that are essential concern of enterprises will be economically available for them. Outsourcing computational needs will reduce costs for organizations because there would not be the needs of the acquisition and maintenance of computing software and hardware used to store and process data, specialist IT staff to manage them, space allocation to keep the equipments, payment for electricity and other energies and payment for maintaining and repairing them.

Cloud service delivery could be commonly categorized in three models i.e. Infrastructure as a service (IAAS), Platform as a service (PAAS) and Software as a service (SAAS) that are explained in following sections in detail.

1.1. Infrastructure as a service (IAAS)

The service provider involves offering, controlling and maintain physical hardware resources such as storage, memory, CPU processing and other fundamental computing resources. This type of service enables customers to deploy and run operating systems and software applications arbitrarily. Allocated computing and hardware resources to customers are metered in order to billing them for their usage. It makes Iaas a suitable choice for various types of businesses to pay for these resources as their use instead of investing on provision of computational equipments.

1.2. Platform as a service (PAAS)

The service provider involves offering Iaas, operating systems and other facilities to the customers and supporting programming languages and tools to enable customers to design, develop, test and implement applications. Controlling and maintaining infrastructure, OSes, tools and other facilities are vendor's concerns. Correspondingly customers only control and maintain their developed applications and probably application hosting environment configurations.

1.3. Software as a Service (SAAS)

The service provider involves offering software applications running on a cloud infrastructure which is accessible through networks from various clients by application users. Customers would not concern about infrastructure and applications which are the responsibilities of vendors. They could be billed for the usage or subscribe monthly for each user. Although aforementioned specifications of public cloud computing make it an appropriate solution for organizations' computational needs, yet various security issues damaged the reputation of public cloud profoundly.

2. MAJOR PUBLIC CLOUD SECURITY ISSUES

2.1. Network Attacks

According to the rest of studies on cloud computing issues, the main challenge in public cloud security is enterprises' data which is stored somewhere in the cloud. In a private cloud, entire infrastructure is under direct control of the owner. In this situation secure protection of the data is applicable by the data owner. However in public cloud data is stored somewhere in the cloud which dedicates data security level profoundly. Moreover in order to alleviate the problem of underutilization of the infrastructure and optimum usage of the computing power and storage capacity, the cloud service providers propose virtual machines to the users. Subsequently a number of customers are running their programs and storing their data on a multi-tenant situation which in this case using of data leakage prevention (DLP) software is worthless to protect the sensitive data. According to this fact, there would be some probabilities in the public cloud for data to be exploited by hackers. A hacker can steal or take under control a virtual machine to host a malicious service or application to attack against service provider or access customer's data [8]. Intercepting the data sent from the client to the server, intercepting and/or spoofing the reply from the server to the client and Launching a DOS attack on the server are the things that an attacker can do using the aforementioned probabilities [17].

2.2. Incompetency of Vendors

In addition to the fact that securing customer's data strategies in public cloud are considerably poor because cloud computing is a new phenomenon in computing industry, many well known companies need to cut their investment on data protection to increase their benefits. Besides minority of customers who have praiseworthy contracts could be under protection of cloud service provider's Enterprise Risk Management (ERM) programs [2]. Moreover many cloud service providers are newly founded companies that do not have adequate understanding about security issues in cloud computing. Disregarding of using secure gateways certified by reliable third party, supporting the cloud service provider's protection method by fragile technical controls and policies, utilizing uncertified devices and products, incapable planning for security incident response and occulting security incidents from customers are various aspects of security issues emerged from the service provider [10]. Additionally incompetency of some vendors causes to data permanence in data store after deletion and non-sensitized legacy storage devices from customers' data. Because of these facts [3] argued that simple faults of service providers such as insecure or incomplete data deletion might make a disaster for data owners. Aside from the vendors and their equipments, their employees are another considerable factor in public cloud security issues. Deploying novice for reducing costs and so on will be very harmful in terms of handling and managing security incidents. Besides neglecting in controlling the employees might persuade wavery ones of them to be hired by attackers to snoop the data. Finally a cloud vendor must be permanently available [16]. That means failure of the vendor will lead to loss of customers' data in some cases.

2.3. Data Access by Vendors

In fact provider access to customer's private data is discussed in many studies that show the significance of this crisis in public cloud environment. Access of service provider to customer's data is undeniable yet cloud storage confidentiality needs to prevent vendor access to user's data [5]. Furthermore loads of other studies specially [19] highlighted data control by service providers as a factor for strengthening security and privacy concerns for customers. More over enterprises with sensitive data still have problems with monitoring privileged access, user authentication and creating business metrics and tracking operational performance on outsourced infrastructure [13]. Access to information by vendors causes to failure of many information privacy protection plans such as: Electronic Communications Privacy Act (ECPA), USA PATRIOT Act (UPA), Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), Video Privacy Protection Act (VPPA), Gramm Leach Bliley Act (GLBA), Cable Communications Policy Act (CCPA) [15].

2.4. Data Access by Government

The concept of cloud comes from uncertain location of infrastructure specially data storage provided by public cloud service providers. Robust international cloud vendors' infrastructures are exploded across several countries with different jurisdictions. It means that the data of an enterprise might be stored in various countries with different regulations and laws governing data storage and data access activities. Therefore geographical data location is the indispensable part of cloud computing. However physical data location and unauthorized access to private data is an apprehension for many enterprises for absence of rules that be globally accepted about data security and privacy [12]. [15] Believed that one of the goals to achieve adequate security is control of the distributed computation over the data in public cloud. The authors also argued that numerous laws in several countries compel public cloud vendors to maintain user data within national borders in

order to make them assessable in law issue point of view. Furthermore [1] believed that public cloud vendors who have full access to customer data which may be stored in various countries with different regulations, may not only hesitate to secure data centers but also set a back door for government snooping.

2.5. Authentication and Virtualization

With considering authentication issues as another drawback of public cloud, risk of cyber attacks could be amplified dramatically. [4] Argued that this security vulnerability allows attackers and hackers to target non-guarded client data over the internet which were hosted in the private data centers previously. They also believed that in public cloud environments which share sources between different subscribers unauthorized access by attackers who posed as subscribers to other's data is facilitated. Sharing infrastructure between customers multiple organizations operating on a vendor's infrastructure are more attractive target than a single enterprise. This fact increases the risk of attack dramatically [2]. [12] argued that even using virtual machines to isolate customers' actions dose not optimize the security of shared infrastructures. Moreover utilizing multi-tenant environments reduce the possibility of investigating offences and crimes.

3. PUBLIC CLOUD SECURITY ISSUES MODELS

In a private cloud-computing environment, the infrastructure is operated and managed on premise and inside the enterprise boundaries. In this type of cloud computing deployment model, company owners have control over the data and processes. However in the case of public clouds, organizations hand over the control to the company owning the infrastructure beyond the designated firewall which is the preliminary point of security concerns for them [6]. It is argued in [14] that effectiveness of the world's standard, no difficulty of utilization by clients and most essentially level of information security are critical success factors for modern technology. Nonetheless security issues and concerns of public cloud are the main anxiety of enterprise owners to move to this useful but challenging environment. Many research papers highlighted the security issues of public clouds for the importance of this fact. For instance, Gartner's model is one of the well-known models that are pointed out about public cloud computing security issues. Gartner classified the important security issues in public cloud to seven points. Different papers focused on it and discussed about it from different points of view such as: [7, 8, 9, 14, 18].

3.1. Privileged User Access

In public cloud deployment model, sensitive data of organizations will be stored and processed over the enterprise boundaries. It is the major cause of high risk.

3.2. Regulatory Compliance

Cloud users are the direct responsible for their outsourced data. Cloud vendors are subjected to external investigations and security certifications.

3.3. Data Location

Many public cloud clients do not exactly know where their data physically store. Cloud service providers usually use distributed data storage method which is unwelcome for clients, especially those who just moved from local data storages to public cloud for lack of control over the location of data.

3.4. Data Segregation

Cloud service providers typically store clients' data beside others'. They use data encryption which is not enough secure to protect users' data as well as possible. Besides it might not be designed and tested by professional experts and available in all stages.

3.5. Recovery

In the case of the cloud server failure or a disaster, customer data will be lost. Dose the vendor offer complete restoration? How long does it take? Besides almost all enterprises do not like a third party company to control their data.

3.6. Investigative Support

Illegal and inappropriate activities are difficult to investigate by service provider, because data and logging for numerous clients might be stored on a same data center and transferred between different physical machines and hosts.

3.7. Long-Term Viability

If Cloud computing provider goes out of business or get acquired by a larger corporation with different rules, how clients could assure that their data will return to them in an adequate format after such an event?

Besides this classification, some other researchers who had studied on this issue classified security problems of public cloud from different perspectives. [11] identified the major problems of public cloud computing and formed a model consist of seven categories that each of them has many security problems:

3.7.1. Network Security

Problems associated with network communications and configurations regarding cloud computing infrastructures (Transfer security, Firewalling, Security configuration)

3.7.2. *Interfaces*

Concentrates all issues related to user (API, Administrative interface, User interface)

3.7.3. Data security

Protection of data in terms of confidentiality, availability and integrity (Cryptography, Redundancy, Disposal)

3.7.4. Virtualization

Isolation between virtual machines, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies (Isolation, Hypervisor)

3.7.5. Governance

Issues related to (losing) administrative and security controls in cloud computing solutions.(Data control, Security control, Lock-in)

3.7.6. Compliance

Includes requirements related to service availability and audit capabilities (Service Level Agreements, Loss of service, Audit)

3.7.7. Legal issues

Juridical concerns related to new concepts introduced by cloud computing (Data location, E-discovery, Provider privilege).

The last type of classifications of security problems in public cloud computing deployment model is proposed by [6]. Following table illustrates the model in detail. As it is shown in the table there are various factors influencing the security issue in public cloud. Each of these factors has its own importance level that is shown in following figure [6].

Table I. Model of security problems in public cloud computing deployment proposed by [6]

User-specific security requirements.

Level	Service level	Users	Security requirements	Threats
Application level	Software as a Service (SaS)	End client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use	• Privacy in multitenant environment • Data protection from exposure (remnants) • Access control • Communication protection • Software security • Service availability	• Interception • Modification of data at rest and in transit • Data interruption (deletion) • Privacy breach • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network
Virtual level	Platform as a Service (PaS) Infrastructure as a Service (IaS)	Developer–moderator applies to a person or organization that deploys software on a cloud infrastructure	• Access control • Application security • Data security, (data in transit, data at rest, remanence) • Cloud management control security • Secure images • Virtual cloud protection • Communication security	• Programming flaws • Software modification • Software interruption (deletion) • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network • Defacement • Connection flooding • DDOS • Impersonation • Disrupting communications
Physical level	Physical datacenter	Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed	• Legal not abusive use of cloud computing • Hardware security • Hardware reliability • Network protection • Network resources protection	• Network attacks • Connection flooding • DDOS • Hardware interruption • Hardware theft • Hardware modification • Misuse of infrastructure • Natural disasters

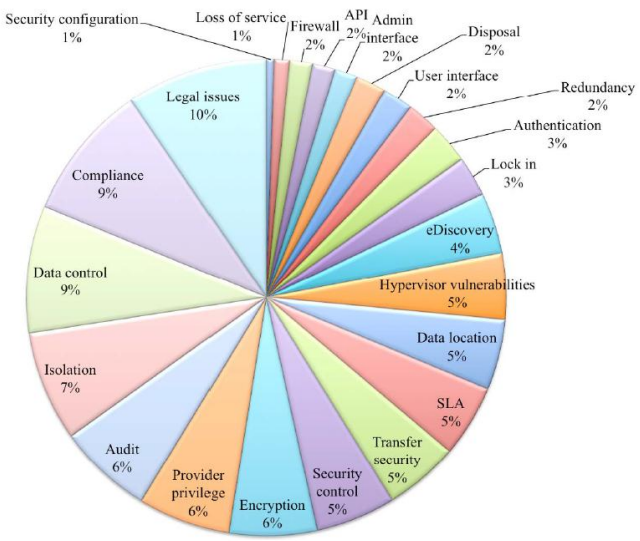

Figure 1. Level of importance of factors influencing the security issue in public cloud [6].

4. CONCLUSION

Although public cloud services enable organizations, governments and even individuals to economically eliminate their computational needs, yet several security issues threat public cloud customers' data. This paper overviewed and discussed the major issues of public cloud computing deployment model. Then it proceeded to discuss proposed public cloud computing security issues models. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. Wherever Times is specified, Times Roman or Times New Roman may be used.

5. REFERENCES

[1] Cheng and Lai (2012). "The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy." Procedia Engineering **29**: 241-251.

[2] Crowe Horwath LLP, Warren Chan, Eugene Leung & Heidi Pili, "Enterprise Risk Management For Cloud Computing", Committee of Sponsoring Organizations of the Treadway Commission, 2012

[3] Fitó and Guitart (2012). "Business-driven management of infrastructure-level risks in Cloud providers." Future Generation Computer Systems.

[4] King and Raja (2012). "Protecting the privacy and security of sensitive customer data in the cloud." Computer Law & Security Review **28**(3): 308-319.

[5] PENG *et al.* (2012). "Secure cloud storage based on cryptographic techniques." The Journal of China Universities of Posts and Telecommunications **19**: 182-189.

[6] Zissis and Lekkas (2012). "Addressing cloud computing security issues." Future Generation Computer Systems **28**(3): 583-592.

[7] Che *et al.* (2011). "Study on the security models and strategies of cloud computing." Procedia Engineering **23**: 586-593.

[8] Sabahi (2011). Cloud computing security threats and responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, IEEE.

[9] Sengupta *et al.* (2011). Cloud computing security--trends and research directions. Services (SERVICES), 2011 IEEE World Congress on, IEEE.

[10] Tripathi and Mishra (2011). Cloud computing security considerations. Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on, IEEE.

[11] Hofmann and Woods (2010). "Cloud computing: the limits of public clouds for business applications." Internet Computing, IEEE **14**(6): 90-93.

[12] Khajeh-Hosseini *et al.* (2010). "Research challenges for enterprise cloud computing." arXiv preprint arXiv:1001.3257.

[13] Orakwue (2010). "Private Clouds: Secure Managed Services." Information Security Journal: A Global Perspective **19**(6): 295-298.

[14] Ramgovind *et al.* (2010). The management of security in cloud computing. Information Security for South Africa (ISSA), 2010, IEEE.

[15] Zhou *et al.* (2010). Security and privacy in cloud computing: A survey. Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, IEEE.

[16] Kandukuri *et al.* (2009). Cloud security issues. Services Computing, 2009. SCC'09. IEEE International Conference on, IEEE.

[17] Muttik and Barton (2009). "Cloud security technologies." information security technical report **14**(1): 1-6.

[18] Brodkin (2008). Gartner: Seven cloud-computing security risks.

[19] Mansfield-Devine (2008). "Danger in the clouds." Network Security **2008**(12): 9-11.

Author's Biography with Photo

Atefeh Heydari, Master Student, Faculty of Computer Science and Information System, UTM, Malaysia-81310, E-mail: a_tav_ir@yahoo.com

Mohammad ali Tavakoli, Master Student,Faculty of Computer Science and Information System, UTM, Malaysia-81310, E-mail: a_tav_ir@yahoo.com

Mohammad Riazi, Master Student, Faculty of Computer Science and Information System, UTM, Malaysia-81310, E-mail: mohammadriazi@gmail.com