Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.502 – 506

RESEARCH ARTICLE

Customer Security Issues in Cloud Computing

Nimmati Satheesh[1]

[1]Assistant professor, PSNA college of engineering and Technology, Dindigul-624224, India

[1] *nimmatisatheesh@gmail.com*

Abstract— The Cloud computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx). In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection-sphere of the data owner. Most of the discussions on these topics are mainly driven by arguments related to organizational means. This paper focuses on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build this cross-domain Internet-connected collaboration.

I. INTRODUCTION

Despite of the fact that industry big players like Google, Amazon, Sales Force, Microsoft and others have products and services under the umbrella of ‘cloud computing’, ‘cloud ready’ or other similar denomination, there is no consensus about what exactly cloud computing is.. It is a new paradigm, not just a distributed computing paradigm, but also a new business paradigm. It is intended to provide computing power, software and storage and even a distributed datacenter infrastructure on demand. In order to make these characteristics viable, cloud computing makes use of existing technologies, such as virtualization, distributed computing, grid computing, utility computing and Internet. However, even those industry big players have products and services available as also a definition of what are the basic cloud computing underlying technologies, a customer intending to better understand and profit from this new paradigm faces several concerns, especially the ones related to security. Considering the customer point of view, we have made an extensive research to obtain what are the main security problems pointed in the available literature for cloud computing security, aiming to list and discuss the more recurrent ones.

II. CLOUD COMPUTING CATEGORIES

Attempts to cloud computing standardization are being done by some groups, including governments and industry. One effort that can help to avoid misunderstandings, by putting everyone to talk the same language, is the definition of cloud computing and its categories. As of this writing, the US National Institute of Standards and Technology (NIST) is one of them, having defined the cloud as composed of four deployment models, three service models and five essential characteristics. The Cloud Security Alliance [6], which formal debut was made at RSA Conference 2009 releasing a white paper entitled “Security Guidance for Critical Areas of Focus in Cloud Computing”, has taken these definitions to work through its guidance, explaining that the motivation is “to bring coherence and consensus around a common language so we can focus on use cases rather than semantic nuance.

A. Deployment models

The definitions of the deployment models listed next are taken as it is from the NIST definition, although other researches mention this deployment models with similar definitions.

1) Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

2) Private Cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party.

3) Hybrid Cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

4) Community Cloud

The cloud infrastructure is shared by several

Organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party.

B. Service Models

There are three service models available in the market.

1) Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications

2) Platform as a Service (PaaS)

"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider [5]."

3) Software as a Service (SaaS)

In this case, is provided "a complete, turnkey application—including complex programs such as those for CRM or enterprise-resource management via the Internet." In each of these service models, what can be controlled by the customer varies, but in general, he does not have

Control over the underlying cloud infrastructure. This is especially true when is the case of a public cloud, the focus of the present paper. In a private cloud, for example, security responsibilities can be taken on by the customer, if he is managing the cloud, but in the case of a public cloud, such responsibilities are more on the cloud

Provider and the customer can just try to assess if the cloud provider is able to provide security.

The five essential characteristics are related on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services.

III. CLOUD COMPUTING SECURITY OVERVIEW

Many cloud computing security problems are still unclear. Being cloud computing such a recent computing paradigm, it is natural that many aspects remain uncovered whereas the paradigm itself is being more

Developed and understood.

Vulnerability to attack: critical business information and IT resources are outside the customers firewall.

Standard security practices: customers want to be confident that such practices are being followed. Most of those practices require disclosure and inspection, which leads to another concern as a customer: will my data be in the same virtual hardware and network resources with other customers, being susceptible to disclosure in someone else's inspection?

Being subject to state or national data-storage laws related to privacy or record keeping:

Permit some personal data to be transmitted outside the EU. In the cloud, data can be stored anywhere in the world; it is important to attend such regulations. Before jumping into the cloud, the customer should know its unique security risks, considering specially seven security conditions during the process of choosing a cloud provider. These unique security risks are:

Privileged user access: outsourcing means allowing outsourced services to bypass internal controls, including personnel controls. With this in mind, the customer has to obtain as more information as possible about how the possible future provider hires people and what kind of controls their accesses have.

Regulatory Compliance: if the cloud computing provider is not subject of external audits and security certifications, the customer probably should not use its services for non-trivial tasks. Customers have to always remember that, unless stated or agreed otherwise, they are responsible for their own data.

Data location: when using the cloud, the customer probably will not know where their data will be stored. Thus, it is recommended checking if the provider will commit to store and process data in specific jurisdictions and if a contractual commitment on behalf of the customer will be made by the provider.

Data segregation: customers should check what is done to separate different customers' provider data, due to the fact that, in a cloud, the environment is shared. Using cryptography, for example, is effective, but do not solve all the problems. It must be checked also if the cryptographic schemes are designed and tested by specialists, because cryptographic accidents are able to make data unusable.

Recovery: the provider capacity of restoring the entire system and how long it would take should be checked by the customer. Any provider that does not replicate its data or infrastructure is prone to total failures.

Investigative support: In order to have confidence that inappropriate or illegal activities will be possible to be investigated, the customer needs a formal commitment

from the provider. This commitment should state which kind of investigation will be possible and also gives evidence that similar support was already done by the provider. Otherwise, the customer almost can be sure that such investigations will be impossible.

Long-term viability: if happens that the cloud computing provider be acquired or goes broke, the customer needs to know if the data will still be available and in a format that will allow being imported to substitute application. Summarizing the Gartner's report, customers should demand transparency and avoid providers that do not

Offer clear information about security. The risks are expected because cloud computing can also be seen as a new business model, with many aspects to be fully understood before being adopted with no restrictions or better, with fewer restrictions. As happen in any new business or technological area, customers and professionals need to be confident on what are they getting into. Storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: Relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. However, users face the situation of losing control of their data. For example, he no longer has physical possession of the outsourced data and may not get to know about data loss and leakage incidents, if the cloud provider for some reason acts unfaithfully and decide not to report the incident just to cite a few.

Cryptography

One could ask if applying some cryptographic and backup schema would not solve at least part of the problem. This is a question certainly being target of studies, especially because as we cited before, cryptographic accidents are able to make data unusable. Trying to contribute to the subject, we bring some questions to this discussion.

- If using cryptography, how the key managements done?

o One key for each customer?

o One key to all customers?

o Multiple keys for the same customer?

- What are the current cryptographic systems more applicable to the cloud computing characteristics especially data storage?

- Last but not least, in which situations

Cryptography should be used?

We think that the cloud provider should have a detailed cryptographic plan, explaining what algorithms will be used, how the key management will be done, when Encryption will be used and so on. The Cloud Security Alliance Guide provides some guidance in these questions. As stated by them, cloud computing divorces components from location and this creates security issues that result from this lack of any perimeter. Hence there is only one way to secure the computing resources: strong encryption and scalable key management. Cloud customers and providers must encrypt all data in transit, at rest or on backup media, since all communications and all storage may be visible to arbitrary outsiders. Customers and providers want to encrypt their data to ensure integrity and confidentiality as also to avoid having to report incidents to their users, remembering that a provider's customer may have their own customer to report and successively. Users are "universally required to accept the underlying premise of trust." highlighting that although some take trust as synonymous of security, it is not and in security the element of trust is more apparent. Relating to the classic key concepts of information security, lists the minimum capabilities that should be offered by the cloud storage provider:

• A tested encryption schema to ensure that the shared storage environment safeguards all data;

• Stringent access controls to prevent unauthorized access to the data; and

• scheduled data backup and safe storage of the backup media.. Such audit would be done by a third-party auditor, called TPA. Knowing that such data in general, due to privacy issues, cannot be subject of disclosure, lists two fundamental requirements for the TPA:

1) Efficient cloud data storage auditing without demanding the local copy of data and without additional on-line burden to the cloud user;

2) No new vulnerabilities should be brought to user data privacy by the auditing process. Such requirements are best practices as also are the reasons mention for the TPA being a good choice instead of the own user auditing the correctness of their data: 1) possible large size of stored data; 2) possible user' computer resource constraints; 3) simply

Downloading the data for its integrity verification is not a practical solution due to the expensiveness in I/O cost and transmitting the file across the network.

Backup and recovery

Backup is probably the more traditional way of keeping data for recovery purposes. However, being crucial to ensure that a point-in-time data is available to restore business operations and given the special nature of a cloud environment, some questions need to be clearly answered by the provider and understood by the customer:

- Who performs the backup?
- How frequent the backup is performed?
- Who is responsible for storing the backup?
- Which backup format is used? Is it dependent of specific technology?
- Logical segregation of data is maintained through the backup execution?

Having these questions being done, another important issue is if the provider will be able to meet any specific customer backup requirement. Normally, to have an effective backup and recovery strategy, a careful study of organization's need have to be done. Being the cloud a multi-tenant environment, it is possible that the cloud provider specific backup and recovery plan will not fit completely to the customer's need. Also, as mentioned before, the data should be encrypted on the backup media.

According to, as a customer and provider of data, it is customer's responsibility to verify that such encryption takes place.

Data format standards

It seems vital to data availability to have a data format that allows customers to take their data from one provider and leverage it inside another provider's application. This kind of concern, however, is neither new or exclusively of cloud computing, so what was already learnt or developed since the beginning of the Internet and the need of data exchange should be taken into account when addressing this situation. The XML (Extensible Markup Language) format was designed to store and transport data. As cited in [13], XML is a technology that started a decade ago and since then great effort has been done by the research and industrial community to support XML and related technologies in RDBMS (Relational Database Management System). Also, being the format subject of standardization and widely adoption, lots of research aiming to secure the format has already been developed and it still is subject of ongoing improvements.

Adopting XML or not, the groups cited here and many others working on cloud computing standardizations should have this in mind: data must be interchangeable.

IV. FINAL CONSIDERATIONS

Cloud computing is a very promising technology that helps companies reducing operating costs while increasing efficiency.

Even though cloud computing has been deployed and used in production environments, security in cloud computing is still in its infancy and needs more research attention. Our paper presents a survey regarding security in cloud computing and Discusses a number of possible research topics to improve security in cloud. We presented an overview of cloud computing, its benefits and classifications. We then discussed security challenges in the current cloud computing model, including both the conventional security challenges that can be applied to cloud computing and a number of new challenges that we think are inherently connected to the new cloud paradigm. Among the current security issues with cloud computing, we emphasized three areas of particular interest, namely SLAs, trusted data sharing, and accountability in the cloud. We have outlined ongoing work on security SLAs for cloud computing, and briefly presented a scheme to address the security and privacy issue in the cloud. As secure data storage in cloud environment is significant concern which prevents many users from using the cloud, we presented a solution to provide security and privacy for user data when it is located in a public cloud. This secure storage solution does not always fit as there are still a number applications that rely on accessing ''clear text'' data in the cloud. We have highlighted the need for further work on accountability mechanisms in public clouds, in order to provide transparent services that can be trusted by all users.

REFERENCES

[1] M. A. Vouk, "Cloud Computing – Issues, research and implementations", In: 30th International Conference on Information Technology Interfaces, pp. 31-40, 2008.

[2] I. Foster, I. Yong Zhao Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", In: 2008 Grid Computing Environments Workshop, pp. 1-10, 2008.

[3] G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT asa Service," IT Professional, vol. 11, no. 2, pp. 10-13, Mar./Apr.2009.

[4] R. Buyya, Y. Chee Shin, S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", In: 10th IEEE Conference on High Performance Computing and Communications. IEEE Computer Society, 2008, pp. 5-13.

[5] P. Mell, and T. Grance, "Cloud computing definition". NIST, June2009, http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html

[6] [6] Security Guidance for Critical Areas of Focus in Cloud Computing, www.cloudsecurityalliance.org (last access on Dec2010).

[7] J. Heiser, and M. Nicolett, Assessing the Security Risks of Cloud Computing. http://www.gartner.com/DisplayDocument?id=685308

[8] http://www.forbes.com/technology/ (last access on Dec. 2010).

[9] http://www.google.com/privacy/privacy-policy.html

[10] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, no. 4, pp. 61-64, July2009

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in2010 Proceedings IEEE INFOCOM. IEEE, March 2010, pp. 1-9.

[12] http://www.dmtf.org/ (last access on Dec. 2010).

[13] R. Zhen Hua Liu Murthy, "A Decade of XML Data Management: An Industrial Experience Report from Oracle", In: IEEE 25thInternational Conference on Data Engineering, pp. 1351-1362.IEEE Computer Society, 2009.

[14] http://www.straffordpub.com/products/cloud-computingmanaging-the-legal-risks-2009-12-09 (last access on Dec. 2010).

