A Review of Data Privacy Issues in Cloud Computing

Mashael Al-zibali
Department of Electrical and Computer Engineering, FOE,
King Abdulaziz University,
Jeddah, KSA

Heba Algethmy
Department of Electrical and Computer Engineering, FOE,
King Abdulaziz University,
Jeddah, KSA

Fatima Bashammakh
Department of Electrical and Computer Engineering, FOE,
King Abdulaziz University,
Jeddah, KSA

Khadijah Jalal
Department of Electrical and Computer Engineering, FOE,
King Abdulaziz University,
Jeddah, KSA

Hemalatha M.
Department of Electrical and Computer Engineering, FOE,
King Abdulaziz University,
Jeddah, KSA

ABSTRACT

Cloud computing has gained substantial research interest and with development, data security issues become more important. The term security has multiple facets such as confidentiality, availability and integrity. A perfect security solution must ensure all the security parameters effectively. With the growing adoption of cloud computing as a viable business proposition to reduce both infrastructure and operational costs, an essential requirement is to provide guidance on how to manage information security risks in the cloud. In this paper, most important security risk to cloud computing is discussed, privacy issue. Finally, a cloud computing framework and information asset classification model are proposed to assist cloud users when choosing cloud delivery services and deployment models based on cost, security and capability requirements.

This paper focuses on the security of data, where the objectives of these various security and privacy related issues and the possible solutions in literature.

Keywords

Data Security, Cloud Computing, ORAM, Data Framework.

1. INTRODUCTION

Cloud computing is a technological advancement for saving user’s data to an external storage system. Therefore, instead of saving data on local user's device, user stores the data on database where internet provides the connection between user computer and the database. Cloud computing has provided “wide acceptance for organizations as well as individuals by introducing computation, storage and software based services. It is used to address the resource scarcity issues of its clients by providing them with on-demand pay-per- use services.” [1]. “Cloud Computing is considered as the modern technology, which developed in last few years, and considered as the next big thing, in the years to come. In last few years, it is grown up from just being a concept to a major part of IT industry. It is likened and equated to the Industrial Revolution in terms of implications for technological innovations and economic growth (Price, 2011)” [2]. Precisely, “Cloud computing is a model for enabling ubiquitous, 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.” [3]. In addition, cloud computing's applications are shown Figure.1 [4].

In recent days, the applications are changing and bigger amount of data is transmitted. Adding modern devices, computers and phones to these services. Therefore, data and application in Internet and mobile have increased. Thus, data must be stored All these technological environments provide new business model which is “data security in cloud computing”. Cloud computing is a very important model solution in recent days and have a lesser cost in order to offers organizations' clouds needed and facilities to accomplish business goals easily. Cloud computing is new service model that offers enormous operation’s cost reduction; unluckily, it has new and unknown risks [5].

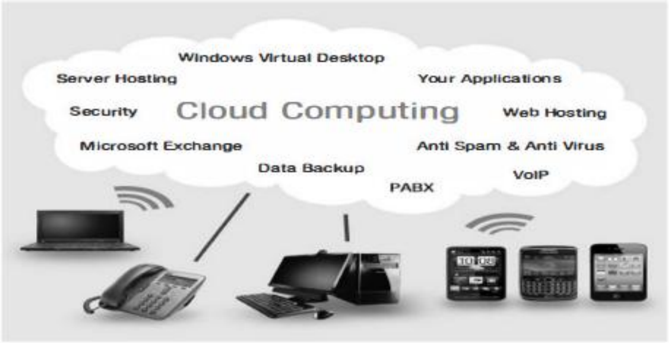

Fig 1: Cloud Computing's Applications and services

2. DATA PRIVACY

In the privacy in the cloud, the researchers have focused on “Oblivious RAM (ORAM)” technology. ORAM is a hopeful technology. So, it used most in the protection of privacy and software in the cloud [6].

2.1 Service Abuse

When the attackers can abuse the cloud service and destroy the interests of other users that are called “Service Abuse”. DE duplication technology is a technology that is extensively used in the cloud storage, that means the same data shared by multiple different users and that data were stored once. This will cause reduce the space of storage and reduce the expense of cloud service suppliers but knowing the hash code of the stored files lead the attackers to access the data. Then, since the responsive data leaks in the cloud. So, "ownership approach" has been suggested to check the certificate of cloud users [7].

2.2 Identity Management

There is a platform that is supplied from cloud computing to use a broad range of services that based on the Internet [8]. But although its features, it also increments the security menace that happens when involving "trusted third party" and that will be as a hole allow the heterogeneity of users, that affects the security in the cloud. The proposed solution for this disadvantage is to use a "trusted third party" separate process for "Identity Management" to use symmetry data on unreliable hosts. To avoid privacy loss and data leakage in the cloud, used different levels of protections [9].

3. RISKS TO CLOUD COMPUTING

3.1 Data Protection

The data privacy is a serious aspect in Cloud computing applications. Data security and privacy have three major challenges that are integrity, authorized access and availability. Data integrity is the assurance that data are uncorrupted and can only be accessed or modified by those authorized to do so. Authorized access is block data from intrusion while backups and replicas allow data access efficiently even when to occur some fault on some location at cloud. So, can prevail hidden proxy applications between cloud and consumer which have user and password to login. There are some solutions for data security and privacy in cloud computing one of them is "Cisco secure Data Center Framework" which is provide multilayer privacy technique [10].

4. CLOUD SECURITY RELATIONSHIP FRAMEWORK

In networks or traditional IT systems, the security management is not like the cloud security management. Like any new technology, unfamiliar risks exist in the cloud computing. To understand the risks and finding appropriate ways of addressing them, conscientious effort must be dedicated. The current situation of the cloud is very immature. Currently, cloud computing deployments are not useful for all cases because of a pay-as-you-go resources, a low cost's gain, and many offerings which adjusted towards adopters with minimizing the risk [11]. The risks with traditional IT should be evaluated to recognize risks correlated with cloud computing. To assist with emerging and new risks concerning the cloud, a framework is proposed. Cloud security relationship framework is defined by Cyril Onwubiko as "a framework for assessing cloud computing offerings (cloud service model, cloud deployment model and use cases) based on cost, security and capability. The cloud computing framework comprises three components, deployment, delivery and user. These components are evaluated against three metrics, cost, security and capability." [12].

The cost depends on the users' pay amount to treat certain cloud service in each deployment. SaaS, PaaS and IaaS are cloud delivery models which provide a specific set of functionalities. The definition of cloud deployment model is a type of cloud computing which offers a coverage set withe uniqueness attributes, e.g. hybrid, public, private, community, localized, and external clouds. Security relates to the availability, confidentiality, and integrity to the cloud computing services. Security offerings in the cloud are difficult to quantify. Therefore, metrics (medium, high, and low) are used instead of mathematical formal metrics usage as which considered by Pfleeger [13].

In the study done, "low security is when one security requirement (confidentiality, integrity and availability) can be achieved; medium security is when two of the requirements are achievable, while high is when all the three requirements can be achieved." [13] .The capability is defined as "the different kinds of offerings available with each cloud computing deployment". Security and cost of the cloud deployment models have direct relationship, like community, public, hybrid, private, and agency. Comparing with hybrid or public clouds, private clouds provide 'pre-requisite' security requirements. The cost grows from public to private clouds for the same type of service, while the cloud's service type capability is directly related. For example, the capabilities of SaaS or PaaS offer less capabilities than infrastructure cloud computing (IaaS). Cloud computing deployment models (community, hybrid, public, private, and agency) offer variety integrity, availability, confidentiality, or privacy of information or data.

4.1 Security Requirements in different kinds of Clouds

"A private cloud is just an owned cloud, operated and implemented by an enterprise. It may be arranged and managed like any other clouds and the most important thing; it is for 'Authorized' users only. Private clouds are more secure than public clouds, and therefore, private clouds are most suitable for sending classified information, such as confidential information. Information assets with minimum-security requirements, such as personal information may still use a private cloud. It is relevant to note that the use of a private cloud offers no guarantee as to the security or privacy of the information assets that it stores or transmitted."

"The companies use the cloud for classified information should use a private cloud. Furthermore, the cost to rent or operate a private cloud is comparably higher than a public cloud. A public cloud is an open cloud maintained by a cloud vendor for the general use of everyone. A public cloud is most probably the most currently used cloud, such as Salesforce, Amazon EC2 and Amazon web services."

"A public cloud is secure and offers a wide range of capability with lesser cost. A community cloud is coordinate by the regulatory controls of that community, for example, health and financial institutions clouds. Agency clouds, like private clouds, are perceived to be secure and reliable because they are privately owned by the military or defense agencies. Hence, complex security requirements are used and implemented. Defense agency cloud may require separate legal, regulatory and security compliance measures different from those of public clouds. These requirements are varying depending on the specific requirements of the co-joining clouds. It is a delusion to think that hybrid clouds provide 'high' security. Each cloud must be assessed in its own right to determine its privacy, security and regulatory policies." [14].

5. FUTURE SCOPE

Cloud Computing is considered the new technology which developed in last years, and it will be a big thing in the future. While technological development to handling the security, concerns is important so, Security data of Cloud computing It can make information technology secure. The future of cloud computing so bright in the several areas. For example:

- Existence of Internet will improve its future making it high speed and secure.
- Software revises for the most part of the computer specialist spend lots of time to downloads the programs so maybe in the future can provide time and efforts for programmer.
- Weather Forecasting: It is supported that with enhanced cover up of computing paired in the company of better climate design it will be perform more comfortable task to weather forecasts.
- Development for all in the field of education.

6. CONCLUSION

Cloud computing have many benefits such as cost savings, quick deployment, and more efficient use of information technology resources. However, there are many problems and one from them is security and privacy of data at cloud computing. The paper presented the issues of security and risks of Cloud computing which are privacy issues and data protection. It has discussed the future scope of Cloud computing.

7. REFERENCES

[1] Sood, S. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), pp.1831-1838.

[2] Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), pp.372-386.

[3] P. Mell & T. Grance, (2011), "The NIST Definition of Cloud Computing. National Institute of Standards and Technology.", US: National Institute of Standards and Technology.

[4] Hosted Cloud Computing, http://www.alchemysys.net/solutions/hosted-cloudcomputing/, 2013. (Access date: 24.08.2013).

[5] "The benefits and challenges of cloud computing", http://www.moorestephens.com/cloud computing_benefits ch allenges.aspxl, 2013. (Access date: 21.08.2013).

[6] Dean, J. and Ghemawat, S. 2008. MapReduce: simplified data processing on large clusters. Communication of ACM 51, 1 (Jan. 2008), 107-113.

[7] E. Stefanov, M. van Dijk, E. Shi et al., “Path oram: an extremely simple oblivious ram protocol,” in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp. 299–310, ACM, 2013.

[8] C. Cachin and M. Schunter, “A cloud you can trust,” IEEE Spectrum, vol. 48, no. 12, pp. 28–51, 2011.

[9] R. Ranchal, B. Bhargava, L. B. Othmane et al., “Protection of identity information in cloud computing without trusted third party,” in Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS ’10), pp. 368–372, November 2010.

[10] K. Hwang and D. Li, “Trusted cloud computing with secure resources and data coloring,” IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.

[11] Cloud privacy: an empirical study of 20 cloud providers’terms and privacy policies—Part I

[12] S. Hussain, "Multilevel classification of security concerns in cloud computing", Applied Computing and Informatics, vol. 13, no. 1, pp. 57-65, 2017.

[13] Pfleeger SL (May/June 2009) Useful cybersecurity metrics. IEE IT Pro J 11(3):38–45

[14] S. Chaudhry, "An Overview On Current Trends, Technologies And Future Scope Of cloud computing", International Journal of Scientific & Engineering Research, vol. 4, no. 8, p. 1888, 2013.