International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 7, No.6 (Nov-2018)

http://dx.doi.org/10.12785/ijcds/070606

The Perception of Information Security Threats Surrounding the Cloud Computing Environment

Heba Mohammed Fadhil[1]

[1]*Department of Information and Communication, Al-Khwarizmi College of Engineering, University of Baghdad*

Received 11 May 2018, Revised 13 Aug. 2018, Accepted 7 Oct. 2018, Published 1 Nov. 2018

Abstract: a form for permitting services to user's everywhere is Cloud Computing; a suitable departure to the network is available upon request for a common set of constructive computing resources. These developments have created new security loopholes, including security issues that remain high full impressions. An up-and-coming area for study is the security of Cloud Computing, in particular for public clouds what can be provided from the infrastructure and computer resources owned by an outsourced party that provides individuals with services. One of the most complex problems in cloud computing is the security challenge. At first security challenges necessitate being addressed ahead of implementing Cloud Computing in an organization. This paper brings out a systematic literature evaluation by spotting the light on cloud computing security necessities; alongside with security issues, it is worth mentioning that solutions for the provision of information security in cloud computing has been discussed in this research.

Keywords: Cloud Computing, Cloud Storage , Cloud Computing Security, Security Threats

1. INTRODUCTION

Let's talk first about the concept, cloud computing allows the use of resources at the highest level and is effective in terms of spending and location sovereign. So that assets are regulated by the seller, such as Amazon, Google, Microsoft, IBM, and zoho; enable the client to use on the cloud. In addition to, its participation in providing tools for programs and on demand various sectors of information technology. Cloud computing features are enormous; it's most distinctive and important is that the customer does not need to buy a supplier by a third party, instead can use the resource and pay for it as a service which saves the customer time and money [1].

The term "on demand" produces an adaptable cloud service, as promising to the end user entrée to a variety of services as per his wish at any time; on the other hand is fully managed by the service provider. To a large extent the achievement of modern technologies in the world depends on efficiency standards, and appropriate consumption through end-users, and furthermost vitally, the amount of information security and mechanism. In terms of providing cloud computing products and services many companies expansion did not properly consider the implications of processing, storing and accessing data

in a common and virtual environment. In reality, many developers are offering cloud-based applications to

embrace safety. In other cases, developers can not fundamentally arrange for real security with currently equitable technological capabilities [2].

Although, cloud computing achievements are particularly attractive but nothing is faultless. The cloud has many problems when it comes to security, especially when data is stolen, data is lost, and privacy is compromised.

These problems are resolved by implementing stronger security measures by identifying challenges and security solutions to identify the correct and efficient treatment methods for these challenges.

This paper is structured within V sections. Section I contributes an introduction to cloud computing. Section II speaks about the structure of the cloud discusses and reviews the pros and cons of the public, private, community, and hybrid clouds, discusses the three cloud computing service models in particulars. Section III discusses the security implications, vulnerabilities, attacks and threats followed by Part IV that places

E-mail address: fadhilheba@gmail.com

interest on how to manage cloud computing security. The closing section is the conclusion that represents in miniature vital results of this evaluation.

2. BASIC CONCEPTS

To make cloud computing effective and available to end users, there are some services and models that work behind the scene.

A. Cloud Architecture

Before digging into security issues, it is imperative to understand cloud definition and architecture. The cloud allows new approaches to deliver products and services through leading, professional and pricing opportunities. There are five factors above all that mainly affect the cloud computing, along with security inferences as described in (Fig.1) [3].

Fig. 2 is a conceptual representation of a complete reference structure for cloud computing. It is important to note that this figure represents an architectural reference to a party by dealing with all seven layers of the model Open Systems Interconnection (OSI), and extends to include commercial and governance aspects. As is evident, cloud computing is a broad cognitive and complex design with multiple ranges of exposure [1].

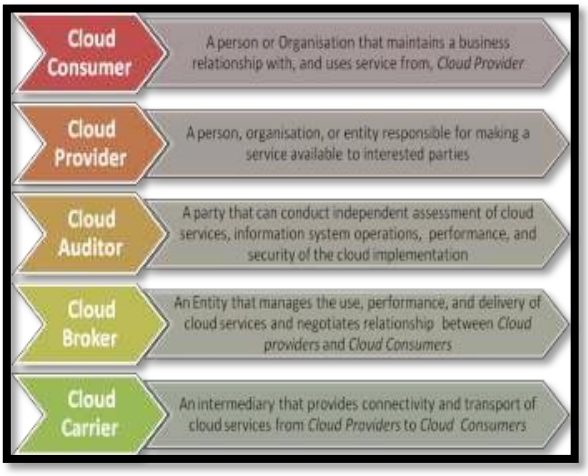

Figure 1. Factors in Cloud Computing Architecture.

B. Cloud Characteristics

Infrastructure carried out by the cloud characteristics, contribute to the deployment of cloud service in terms of cost is in fast and efficient manner. In addition, cloud computing devises a range of properties, and the furthermost main are [4]:

- ***Shared Infrastructure:*** consumers can unilaterally provision computing capabilities by approving the participation of physical services, storage and networking abilities; such as network storage and server time, as desirable inevitably without necessitating human interface per every single service provider.
- ***Dynamic Provisioning:*** with the network, capacity is provided and edited based on up-to-date demand necessities. This is finished inevitably through standard mechanisms deployed for use through heterogeneous client platforms as needed. Alteration of this dynamic procedure must be done even though preserving extraordinary levels of consistency and safety.
- ***Network Access:*** A wide range of different physical and virtual resources that must be accessed via the Internet through dynamically installed and reset according to the request using programming interfaces standards-based applications (for instance, those established on HTTP). Cloud deployments also embrace everything from using business applications to the latest applications on the cutting-edge smartphones.
- ***Rapid Elasticity*:** A measure is used to manage and improve the service and provide reporting and billing information. In this way, consumers are invoiced for the services according to how much they actually used during the billing period. In short, cloud computing allows the sharing and scalability of services, as desired, from just about anywhere, plus invoicing to the customer founded on their concrete use can be achieved [5].

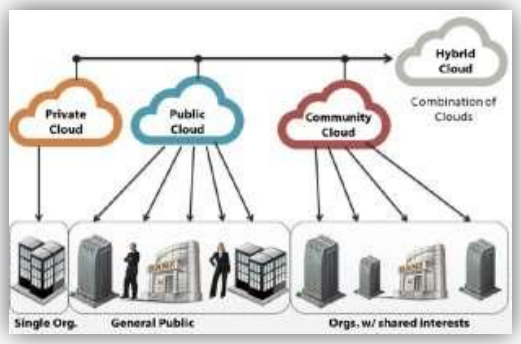

Figure 2. Cloud Computing Reference Architecture [1].

C. Deployment Models

Diverges deployment of cloud computing on the basis of requirements; In addition, there are four well-known deployment models, each of which has certain characteristics needed to support facilities besides users of the cloud in certain means (see Fig. 3) [6].

1) Public Cloud

The cloud relies primarily on allowing systems and services to be accessible to the public without any problems; such as applications and storage. In addition it may be less safe because of its validity. Free public cloud services may be accessible in a pay-per-use form. Nominal profits from the use of public cloud service are:

- Effortless plus low-cost setup, since costs are enclosed through the supplier.
- Scalability to convene needs.
- Certainly not exhausted resources are given as you pay for what you use.

2) Private Cloud

The **Private Cloud is** a proprietary computing architecture to facilitate hosted services to be easily reached inside an organization at the rear of a firewall. It offers improved security for the reason that of its reserved nature.

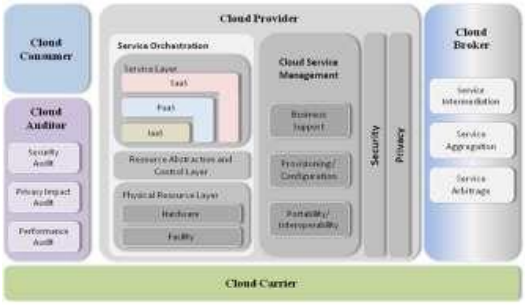

Figure 3. Cloud deployment models.

3) Community Cloud

Community Cloud systems allow collective systems and services amongst an amount of organizations through related concerns and necessities. Asset expenses establishment costs could be limited because of the common costs between the organizations. Organizations or a third party can manage them as well as may exist on premise or off the platform.

4) Hybrid Cloud

Hybrid Cloud It's a hybrid of at least one private cloud in addition to one public cloud. However, vital activities are carried out using the private cloud, while non-biological activities are carried out using the general cloud. Thanks to the hybrid advance of the business that can take advantage of the scalability and cost suitable for the general cloud by means of the current computing environment avoids exposing applications and data critical to the task of external security gaps [6].In Figure 4, security matters associated to deployment models for private plus public cloud computing plus hybrid cloud are presented. Subsequently the pros and cons of expending these published models ought to been itemized as well [5].

Figure 4. Positives deployment model with the security level and disadvantages.

D. Cloud Service Models

Cloud computing requirements development of computing resources (servers, storage and applications): as services for the end user through the cloud service providers. Those end users are turning to demand for cloud services across web browsers. The provision of micro-cloud services by cloud computing service providers; also guarantee the quality of services.

Cloud computing generally embraces three layers: the application layer, the platform layer, and the system layer. The system layer is the base layer, which embraces computing resources, for example, server infrastructure, network devices, memory, and storage. It is recognized as Infrastructure as-a-service (IaaS). Computing resources are provided to users as services on demand [3]. Through the use of virtualization technology, it allows customers to build complex infrastructure networks through virtual machines provided by IaaS. This technique not only reduces the cost of buying physical equipment companies, but it reduces the burden of network management because IT experts are not obliged to monitor the health of the physical networks continuously [6].

A model on the cloud computing service provider for IaaS is EC2 in Amazon. It provides virtual computing environment in the company of web service interfaces. Through the use of interfaces, users can deploy virtual machines based on Linux or Solaris or Windows and run their own custom applications. The platform layer is the central layer also known as Platform-as-a-Service (PaaS). To design applications

for users; is a creative platform to deliver development. This model offers a number of cloud services that contain tools and libraries to develop applications, which control feature gives users the deployment of applications and configuration settings. By PaaS, developers are not required to purchase software development tools; resulting in low cost.

An example of PaaS is Google Apps; as it is made up of Google tools that include Gmail, Calendar, Groups, Sites, Talk, and Docs Group. Counter users to convert these tools to their own domain names. One of PaaS providers is Windows Azure. This paves the way for users to build applications through a variety of languages, tools or frameworks. After that users can join the applications in IT environments that can be obtained [7].

Lastly, the superior level is the applications layer, correspondingly recognized as software as a service (SaaS). This layer permits users to lease applications running on the cloud as an alternative to paying for the purchase of these applications. Since its establishment to reduce costs, SaaS has become popular amongst the companies that publish its business. Groupon uses an instance of SaaS. With the use of Groupon online support solutions, Zendesk processes thousands of daily customer tickets more efficiently as a result of better customer service. Marathon data systems are one more illustration that displays SaaS. Figure 5 shows examples of specialized providers of cloud computing services in three models of cloud service [8].

3. INFORMATION SECURITY IN CLOUDS

The main objective of the cloud is to provide computing resources on demand - everything from applications to data centers - on the basis of online pay-per-use. The cloud includes the advantage of reducing capital costs and improving accessibility and flexibility. Despite its advantages, there are many security effects, the most serious of which is information security in the cloud. They are many of the security implications that are focused on serious issues are summarized security issues as follows [7] [8]:

1) **Security of individuals: w** ith personal security, an organization appoints authorized individuals or a group of individuals to access all resources, data and allocation.

2) ***Eavesdropping:*** unauthorized user can access the data due to interception in the network traffic, it may lead to failure of secrecy. The listener secretly listens to a private conversation to others. This attack can be done via e-mail, instant letters, etc.

Figure 5. cloud computing service providers.

3) ***Information security: w*** ith information security, the organization can protect confidentiality, health (Integrity) and asset information for processing and storage.

4) ***Physical security: w*** ith this security, the organization can protect its physical assets and other basic characteristics of unauthorized access and misuse.

5) ***Network-level security: w*** ith network security, the organization protects network and communication components. It's also Protects the contents of the organization that are transferred through networks.

6) ***Security operations: w*** ith operational security, the organization protects the information from all transactions and processes perform regularly.

7) ***Communication security: w*** ith the security of communications, the organization protects various technologies and communications media and their content of unauthorized access [9].

4. TREATING CLOUD COMPUTING SECURITY ISSUES

There is an urgent need for advanced techniques and concepts of extensive and sophisticated methods and provide a safe servant leads to a secure cloud. In order to activate the operative use of cloud computing technology, the research community needs to take practical and positive measures to ensure security and

ensure compatibility between service providers [10]. Expand security standards to justify the confidentiality of data, integrity, and availability, together incorporate into this effort. Conversely, the following are a number of the most excellent practices in the field of counter measures and controls the measures that could be considered [1] [2] [8]:

1) ***Encryption of end-to-end***: Data may pass through a cloud delivery model across multiple positions; it is necessary to encrypt data from end to end.

2) ***Look for harmful behaviors:*** Encryption from end to end although strongly endorsed, drives a new risk, also cannot read the data encrypted by means of the firewall. For this, it is necessary to have adequate controls and countermeasures to reduce the risk of malicious software passing through encryption [11].

3) ***Cloud consumer authentication:*** The cloud provider should adopt adequate precautions to check the cloud user to ban the important features of the cloud used to attack targets deceptive.

4) ***Secure interfaces and application programming interfaces (API):*** interfaces and programming interfaces are considered very important applications for the automation and management. So the cloud provider must make sure tempering any weakness.

5) ***Attacking from inside***: The duty of the cloud service providers to adopt the necessary testing employees and contractors precautions, as well as the strengthening of internal security systems to avoid any internal attacks.

6) ***Securing subsidized resources:*** In mutual multi-user model, includes a cloud service provider to secure a common source, such as administrator, harmony and monitoring tools.

7) ***Business permanence strategy:*** Continuity project activity is the codification of the organization in response to any incidents causing the entire deficit or part of the vital work processor process [9] [12].

REFERENCES

[1] G. Ramachandra, M. Iftikhar, and F.A Khan, "A Comprehensive Survey on Security in Cloud Computing ", *Procedia Computer Science*, *110*, pp.465-472, 2017.

[2] O. Harfoushi, B. Alfawwaz , N.A. Ghatasheh, R. Obiedat, M.M. Abu-Faraj, and H. Faris, " Data security issues and challenges in cloud computing: a conceptual analysis and review," *Journal of Computer Science & Communications*, pp.15-21, 2014.

[3] S. Goyal, " Public vs private vs hybrid vs community-clo computing: a critical review," *International Journal of Computer Network and Information Security*, *6*(3), p.20, 2014.

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

[5] F.F Moghaddam, M.B. Rohani, M. Ahmadi, T. Khodadadi, and K. Madadipouya," Cloud computing: Vision, architecture and Characteristics," In *Control and System Graduate Research Colloquium (ICSGRC), 2015 IEEE 6th* (pp. 1-6).

[6] H.M. Musse, and L.A. Alamro, " Cloud Computing: Architecture and Operating System," In *Computer & Information Technology (GSCIT),2016 Global Summit on* (pp. 3-8).

[7] A. Girma, M. Garuba, and J. Li, "April. Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics," In *Information Technology-New Generations (ITNG), 2015 12th International Conference on* (pp. 206-211).

[8] E. Aruna, A.A. Shri, and A. Lakkshmanan, " Security concerns and risk at different levels in Cloud Computing," In *Green Computing, Communication and Conservation of Energy (ICGCE), 2013International Conference on* (pp. 743-746).

[9] F. Ahamed, S. Shahrestani, and A. Ginige, " Cloud computing: security and reliability issues," *Communications of the IBIMA, 2013*, p.1.

[10] K. Hashizume, D.G. Rosado, E. Fernández-Medina, and E.B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, *4*(1), p.5, 2013.

[11] R.V. Rao, and K. Selvamani, " Data security challenges and its solutions in cloud computing," *Procedia Computer Science*, *48*, pp.204-209,2015.

[12] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A.V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Information Sciences*, *258*, pp.371-386, 2014.

Heba M. Fadhil, Msc. was born in Baghdad, Iraq, in 1984. She received the B.E. degree in computer engineering from AL-Mustansryia University, Iraq, in 2006, and the Master degree in Computer engineering from the University of Baghdad, Collage of Engineering, Baghdad, Iraq, in 2014. In 2006, she joined the Department of Information and Communication, Al-Khwarizmi College of Engineering, University of Baghdad, as a senior engineer, and in 2014 she became a lecturer. Her current researches interests include are cryptography algorithms, parallel processing, operating systems, data structures, object oriented technology, artificial intelligence and image processing. Ms. HEBA is a fellow member of Association for Computing Machinery (ACM) and the International Association for the Engineers; also is editorial board members of the International Journal of Applied Science and Technology Research Excellence, and is A Reviewer in Journal of Computer Science, International Journal of Engineering Research and Technology (IJERT), ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data (IITCIB), International Journal of New Computer Architectures and their Applications, Circulation in Computer Science Journal.