World Applied Sciences Journal 35 (8): 1252-1256, 2017
ISSN 1818-4952
© IDOSI Publications, 2017
DOI: 10.5829/idosi.wasj.2017.1252.1256

A Perspective of Cloud Computing: Data Threats and Challenges

Ahmad Faisal Abidin, Suhailan Safei, Mohamad Afendee Mohamed and Nor Surayati Mohamad Usop

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Malaysia

Abstract: The Cloud computing enables a pool of virtualized computer assets to be computed and managed in a centralized environment. A cloud is capable of hosting different workloads and can actually allow workloads to be deployed/scaled-out on-demand by the rapid provisioning of the physical or virtual machines. Also, the cloud is able to support the self-recovering model which permits workloads to recuperate from software and hardware failures and rebalance allocations. Considering the global growth of the Internet, cloud computing has no doubt promoted the exponential expansion of computing and storage capabilities. Various applications can be run on the remote servers without the monotony of local installation and maintenance. Furthermore, cloud computing structure empowers a centralized storage, software applications, memory, processing power and speed through good bandwidth among the interconnected machines. The concept behind cloud computing is the transfer of desktop computing to a service-oriented platform that makes use of server clusters and dispersed storage. This paper provides in-depth analysis of the cloud computing structure and lastly, the challenges and threats of cloud computing and the security issues will be discussed for some potential future research perspective.

Key words: Cloud Computing · Cloud Security · Cloud Services · Cloud Models

INTRODUCTION

The computer is a life-changing technology which has evolved tremendously over a short period of time. It has unbelievably wiped various manual tasks from the simplest ones to highly complex ones out of human shoulder. The computer which initially allowed individuals to work at home and later in groups connected as a small office network has now become the largest spider web-like connections ever [1-2]. There is nothing new about humans sharing their intellectual and memory capabilities to solve real-world problems. Similarly, computer power and storage can be grouped together to offer a highly capable computing power for solving many complex real-world problems. Conceptually, sharing the computing resources and offering them to customers is similar to offering utility services such as water, gas and electricity. Cloud computing is another newly born commodity that is controlled by a cloud provider and is reaching out to users at every corner of life [3].

Cloud computing has to do with the collection of extant technologies and techniques that are bundled in a new infrastructure paradigm which offers elasticity, improved scalability, lowered management costs, business agility and faster start-up time with the little available time. [4]. Cloud computing is accessing computing resources as a service rather than a product using shared software. Platform and infrastructure as a service are provided to computers and other devices as a utility over a private as well as public network.

Cloud computing is an on-demand Internet-based or intranet-based architecture through pay per usage mechanism by pulling shared resources which includes applications, networks, services, individuals and servers without the physical acquisition of these resources [5]. Thus, the platform minimises the cost and time of an organisation in managing hardware and software resources. Many institutes such as educational, banking and healthcare have almost adopted cloud computing for the betterment of their service efficiency. Also, cloud computing enables organisations to meet the needs of the rapidly evolving markets easily thereby making sure that they are always the best choice for their customers. It is one of the important necessities of every business considering the fact that the users can make use of the infrastructure without managing it and also without

Corresponding Author: Ahmad Faisal Abidin, Faculty of Informatics and Computing,
Universiti Sultan Zainal Abidin, Besut Campus, 22200, Terengganu, Malaysia.

organisational manpower. Although the concept of cloud computing was initially available in academic fields only, however, things have changed because it has recently been spread to industries by companies such as Google, Microsoft, Yahoo, Snapdeal and Amazon. This implies that new start-ups can now enter the market easily because the cost of infrastructure has greatly reduced. This allows developers to concentrate on the business value rather than on the starting budget.

Cloud Structure: In this section, we expose readers to the underlying structure of cloud computing. Focus will be given to the introduction of the interested and involved parties in the cloud computing, various models on how cloud computing service can reach out to the customers from providers and different types of deployment according to the target customers.

Cloud Computing Entities: In cloud computing network, there are four interested parties that are directly involved in the business, namely cloud providers, cloud consumers, cloud service brokers and cloud resellers [6]. Cloud service consumers and cloud service providers are two major entities identified in the cloud computing business environment. However, there are also two new emerging service level entities that can be identified in cloud computing which includes cloud service resellers and cloud service brokers.

The three main pillars of cloud service providers include telecommunication companies, Internet service providers (ISP) and large business processes that provide the media and infrastructure which allows consumers to access cloud services. Fundamentally, the end users are cloud consumers, however, resellers and cloud service brokers may also be part of this category the moment they are consumers of another broker, reseller or cloud provider.

The cloud service brokers include registered broker agents, technology consultants, influencers and professional service organisations. The good relationship between service providers and consumers is managed by service brokers though they do not manage the entire cloud infrastructure.

Presently, cloud resellers are increasingly becoming an important part of the cloud market while the providers expand the scope of their business across the world. Those that cloud providers choose to serve as resellers of their cloud products in their respective fields include resellers of existing products, agencies and local IT consultancy firms.

Different Models of Cloud Computing: By definition, model defines the abstraction of the real-world problem. Cloud services can reach up customers at three different abstraction levels. This abstraction level determines how transparent the service is to the users. Cloud services can generally be classified into three abstraction level [7].

Software as a Service (SaaS): This service is a distribution model of various services where applications are being hosted by service providers or vendors and made available and accessible to consumers via the internet. SaaS is actually one of the widespread delivery models with basic technologies that support both web services and also service-oriented architecture.

Platform as a Service (PaaS): PaaS is a service that has a set of software and development tools that are hosted on the provider's server. Not only is it one layer above IAAS on the stack but it also abstracts everything up to the operating system. It creates an integrated set of developer environment which allows developers to build their applications even when they have no clue regarding what takes place underneath the service. It provides developers with a complete software development lifecycle management service which starts from the planning stage to design, building of the application, development, testing and maintenance.

Infrastructure as a Service (IaaS): As a single tenant cloud layer, this service allows only contracted clients to share the dedicated resources of the cloud computing vendor on the basis of pay-per-use. It minimizes the need for clients to invest in computing hardware like processing powers, servers and networking equipment.

Cloud Deployment Model [8]: Cloud deployment can be classified into four different models. The main cloud service Deployment Models are as follows:

Private Cloud: A private cloud can be leased and managed by a third party or an organisation at "on-premises" or off-premises" of the organization. Comparatively, it is more expensive, however, it is also more secure than other clouds. The public cloud environment has no extra-legal requirements, bandwidth limitations or security regulations. While making use of a private cloud service, both the clients and the service providers have actually optimized control of the infrastructure and also ensured that the security of the cloud is greatly enhanced.

Public Cloud: As a cloud infrastructure, it provides services to several customers while being managed by a third party that exists beyond the organisational/company firewall. A number of enterprises execute their task at the same time on the infrastructure and the users can enthusiastically stipulate resources. This type of cloud is totally hosted and also managed by cloud providers whose duties involve installation, management and maintenance. Due to the fact that consumers have limited control over this cloud, they are charged only for the resources they utilize. Public clouds do not really require powerful security and regulatory compliance. There will not be any access restrictions when using this model and also, authorisation and authentication techniques will not be used. Some examples of good public clouds include Google App Engine and Microsoft One Drive.

Hybrid Cloud: This is the combination of two or more cloud deployment models that are linked in mesh topology which ensures that the data transfer occurs between them without having any effect on each other. This model of clouds are typically shaped by management endeavour and responsibilities and would usually split between the cloud service provider and the enterprise. A company is able to outline the needs and goals of its services in the hybrid cloud model and a well-constructed model can be highly useful for providing secure services like receiving customer payments and also those that are secondary to the business like the processing of employee payroll. However, a major challenge with this model has to do with the difficulty in being able to effectively create and override such a solution. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Community cloud is a shared Infrastructure by several organisations for a shared reason which is often managed by the organizations or even any third party service provider. This cloud model is rarely offered and they are mainly based on an agreement that takes place between particularly similar business organizations like banking and educational organizations. An example of a Community Cloud includes Facebook, Twitter etc.

Cloud Security: In essence, security is about securing data from being read by the unintended recipient. Data security has evolved from securing static data in a computer system, to mobile data under transmission from a computer to another in a network of local computers to an internet size of network. To this point, data is communicated to the recipient who the data is meant for and purely legit to open and read it. Slightly different, cloud security is about securing data from being read by whom it was sent for, to the least other than attackers. In reality, the data was intended for a computer processor, not for human recipient. The data should go through certain processes and return back to the sender in a form of output. However, in doing so, the data need to be in readable format. Therefore, whosoever has an access to cloud networks or computers are free to open and read the data. The issue is now, how do we protect our data from being read by someone with a legit access to the cloud network as well as attackers who managed to hack into the network. Security inside cloud computing is a major challenge since the devices used in the provision of the services are not owned by the users.

Key Security Issues in Cloud Computing [9-10]: Cloud security is the cloud computing security issues which range from the hardware assets (e.g. system virtualization, network and communication), software resources (e.g. application programming, data) and business/legal issues (e.g. service level agreement, governance, vendor lock-in). Different operations are carried out by each segment and each segment renders different types of products for individuals and businesses around the world. As the damage caused by security attack on hardware and business can be fixed, data damages or breach in the cloud computing environment can be considered as a most serious threat due to how difficult it is for the data to be recovered or restructured.

Challenges of Cloud Security: It is believed that the main reason behind cloud security is end user's awareness [11]. The end user should be aware the potential of data loss or theft when it is stored in an online environment. It is also possible that the data at a certain time cannot be accessed due to the inconsistent network connection issue. The users who are not familiar with cloud security standards may be easily attacked with security issue without having their own protection. Some issues are mounting at service Level Agreement as the data is available at that end. Costing model and charging model are also one of those challenges of today's cloud security. The survey of cyber security on cloud computing discovered that performance and security risks were identified in 99% and 97% of the environments respectively and also 82% of companies were facing data loss [12]. The end user's issue is not only related to individuals, but also happen to many organisations. The results of a survey of more than 290 IT professionals located in nine different countries which includes: Canada, US, China, Japan, France, UK, Germany, India and Mexico, suggests that a total of 26 percent of organisations surveyed are either "somewhat confident" or "not confident" regarding the level of knowledge of their IT teams in using all cloud storage providers. Also, it was discovered that about 15 percent of organisations surveyed never or rarely carry out the audits of their cloud providers in charge of storing their corporate data. The organisations that confirmed their ignorance of the security precautions that should be taken to prevent the loss/theft of data while a cloud/virtual server is being decommissioned/shut down was 16 percent. Approximately two-fifths (40 percent) of organisations believe that storing corporate data in a cloud environment increases their compliance and confidential risk.

Some Solutions for Cloud Security [13]

Consumer's Loss of Control: Applications, resources and data are actually located with the provider so the chance of loss of data may occur anytime. The user access control rules, security policies and enforcement are managed by the cloud providers and they are always a risk Client identity is also managed and controlled in cloud so the loss of data is a risk. The provider must be monitored at the local end by some specialised organisations. The customer should be utilizing different clouds and there must be access control management at organisation level.

Lack of Trust (Mechanisms): If there is a deviation in the conversation, then the lack of trust will always take place. The definition of trust (reliable) and risk (unreliable) must be known. The standard language to convey all policies and expectations should reach the end user. The creation of policy language must take place. The certification of a service provider is mandatory and risk assessment should be reviewed timely.

Multi-Tenancy: When there is a conflict between tenants' opposing goals, the separation between tenants and multi-tenancy deal with conflict of interest occurs in providing services. The organisation must try to increase isolation between tenants.

DISCUSSION

Security countermeasures can be in many forms such as legislation and laws, standards and policy and technological tools such as hardware and software devices. In general, we can summarise using the following points. An organisation should be aware of and understand the procedure and protocols about what, when and how the data is stored and when it needs to be removed from the provider's side. On top of that, while data is stored offsite with a cloud provider, the organization needs to be aware of the data storage location. Every organisation should at least once every year strictly carry out the audits of cloud providers that store their corporate data so as to assess their integrity and capability of handling the data. Finally, cloud compliance should include and revise the security policies and also procedures being applied by the storage provider to data For future research direction, it will be good if end users can protect their own data before storing them on the cloud environment. Offline protection mechanisms or approaches that are user-friendly can be further explored not only to protect the data but also to increase the awareness of data security among the end users.

CONCLUSION

Sharing of resources happen to be among the greatest security challenges associated with cloud computing model. It is important for customers to be properly informed by the service providers about the extent to which they can provide security on their cloud. Another major issue facing cloud computing is data security. There exists several security challenges which include the security aspects of network and visualization. These issues facing cloud computing were highlighted in this paper. Cloud computing is faced with several challenges due to its complexity and definitely, it will be tough to really achieve end-to-end security. Organisations should adopt the latest security techniques while properly maintaining the older ones to ensure that they work effectively with the architecture of the cloud.

REFERENCES

1. Zhizhong Zhang, Chuan Wu and David W.L. Cheung, 2013. A survey on cloud interoperability: taxonomies, standards and practice. SIGMETRICS Perform. Eval. Rev., 40, 4 (April 2013), 13-22. DOI: http://dx.doi.org/10.1145/2479942.2479945.
2. Saurabh Singh, Young-Sik Jeong and Jong Hyuk Park, 2016. A survey on cloud computing security: Issues, threats and solutions. Journal of Network and Computer Applications, 75: 200-222.

3. Crago, S., *et al*., 2011. Heterogeneous Cloud Computing, 2011 IEEE International Conference on Cluster Computing, Austin, TX, 2011, pp: 378-385. doi: 10.1109/CLUSTER.2011.49
4. Satyakam Rahul and Sharda, 2013. Cloud Computing: Advantages and Security Challenges. International Journal of Information and Computation Technology, 3(8): 771-778.
5. Troppens, U.L.F., *et al*., 2011. Storage networks explained: basics and application of fibre channel SAN, NAS, iSCSI, infiniband and FCoE. John Wiley & Sons, 2011.
6. Sheikholeslami, Fereshteh and Nima Jafari Navimipour, 2017. Service allocation in the cloud environments using multi-objective particle swarm optimization algorithm based on crowding distance. Swarm and Evolutionary Computation.
7. Piraghaj, Sareh Fotuhi, *et al*., 2017. "A survey and taxonomy of energy efficient resource management techniques in platform as a service cloud. Handbook of Research on End-to-end Cloud Computing Architecture Design, pp: 410-454.
8. Jain, Abhinivesh and Niraj Mahajan, 2017. Introduction to Cloud Computing. The Cloud DBA-Oracle. Apress, pp: 3-10.
9. Naim Ahmad, 2017. Cloud computing: Technology, security issues and solutions. Proc. of IEEE 2nd International Conference on Anti-Cyber Crimes (ICACC), 2017.
10. Hamlen, Kevin, *et al*., 2012. Security issues for cloud computing. Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies, pp: 150.
11. Ertaul, Levent, Sarika Singhal and Gökay Saldamli, 2010. Security Challenges in Cloud Computing. Security and Management.
12. Blanco, 2016. Lost in the Cloud: Data Security Challenges & Risks.
13. David Turahi, 2013. Security and Privacy: Can we trust the cloud?” East African Information Conference, Kampala, Uganda.