International Journal of Computer Science and Software Engineering (IJCSSE), Volume 7, Issue 11, November 2018
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 260-263

Trust in Cloud Computing: Concepts, Issues, and Challenges

Faisal Babtain[1] and Dr. Abdelrahman Karrar[2]

[1, 2] Faculty of Computer Science and Engineering, Taibah University, Madinah, Kingdom of Saudi Arabia

[1]faisal-h.b@hotmail.com, [2]dr.elsharif@hotmail.com

ABSTRACT

Cloud Computing is emerging today as an infrastructure that removes the need for preserve expensive computing hardware. Cloud Computing is a new model to enable convenient and on-demand access to the grouping of configurable computing resources. Cloud Computing is a set of IT services that are provided to a client through a network and with the capability to scale up or down their service requirements. Generally, Cloud Computing services could be delivered by a third party supplier who has the infrastructure. Trust is one of the essential issues, which constraints the growth of cloud. Trust in the Cloud Computing is a critical issue and it is one of the most challenging issues in the cloud. Therefore, this research aims to define the trust, issues, and challenges in Cloud Computing.

Keywords: *Trust, Cloud Computing, CloudX, VM protection*.

1. INTRODUCTION

Cloud computing offers a network of interlinked computer and device systems that can be quickly controlled with minimum efforts in management. Usually, the practice is performed over the internet. With various computing services, it provides a wide range of opportunities to the enterprises. In the current competitive environment, the elasticity, the service dynamism, and choices offered by this technology that is quite scalable, these are too efficient to be ignored by the enterprises. However, such opportunities don’t come alone. They rain down with a shower of challenges as well. In this article, the meaning of trust together with its establishment in it are discussed. Furthermore, the challenges faced with their solutions are also confronted in this article [1].

Cloud computing opens a new door for the enterprises by offering various computing opportunities and services. The environment today is indeed quite competitive. So, when this efficient technology offers several choices, dynamism, and elasticity, enterprises cannot help but turn to it. However, opportunities never come alone, they have challenges in the pocket as well [2].

A new package of challenges has been offered by cloud computing in the form of different trust scenarios. For many enterprises, putting trust in cloud computing has become a significant concern. Enterprises don't doubt the service providers of the cloud. They question the capabilities of the cloud. Still, such challenges don't depend entirely on the technology. The lack of consumer confidence also emerges from the smudgy security assurances, loss of data, and less transparency.

Nowadays, the number of cloud users and adopters has been dramatically increased. Cloud Computing has been widely considered and used by individuals and organizations. Its exceptional features such as smooth access to a shared pool information, lower entry cost and pricing has encouraged information technologies leaders to adopt Cloud Computing in their business. Several studies have been conducted on such domain. Consequently, most of these studies have identified that trust of Cloud Computing is the most challenges, which in turn needs to be addressed [3].

To close the gap between the consumers and cloud computing, it is necessary to understand the trust problems first. The problem is that there is no trust or confidant of storing data on clouds for some consumers. Moreover, there is a large number of organizations contain important and sensitive information. So, they need to secure and maintain these information.

2. CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) defined Cloud Computing as "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 is composed of five essential characteristics, three service models, and four deployment models." [3].

According to NIST, there are many attributes of Cloud Computing which enhance enterprises and individuals to trust on Cloud. The essential attributes are On-demand service, Broad network access, Resource pooling, Rapid elasticity, Measured services [3].

Cloud Computing has two types of models, which are Deployment Models, and Service Models. Deployment models divided into four sections that are Private, Public, Community, and Hybrid.

- Private cloud

  A private cloud provides more security than public clouds. It is set up within an organization‘s internal enterprise data center. The scalable resources and virtual applications provided by the cloud vendor are merging which are available for cloud users to share and use. The use of private cloud can be much more secure than that of the public cloud [3].
- Public cloud

  A public cloud is a publicly accessible cloud environment owned by a third-party cloud supplier. The IT resources on public clouds are usually provisioned by the previously described cloud delivery models and are commonly offered to cloud consumers at a cost or are commercialized via other avenues (like advertisement) [3].
- Community cloud

  A cloud infrastructure shared by several organizations with shared concerns loud except that its access is limited to a specific community of cloud consumers. The community cloud may be jointly owned by the community members or by a third-party cloud provider that provisions a public cloud with limited access [3].
- Hybrid cloud

  Hybrid Cloud is merged both private and public cloud to execute characteristic functions within the same organization. It can also be defined as multiple cloud systems that are connected in a way which allows programs and data to be moved easily from one system to another. It is a configuration of at least one private cloud and at least one public cloud This computing model combines the security benefits of a private cloud as well as the public cloud [3].

  On the other hand, Service model has three primary sections which are Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a service (PaaS). Also, it has another services as secondary services such as Data as a Service (DaaS), Identity and Policy Management as a Service (IPMaaS), and Network as a Service (NaaS).

3. MEANING OF TRUST

Trust is the strength of confidence and faith in something. The spirit seeks the results that are expected to be produced by something. It is the belief in the expertise and talent of others to care for the person and develop satiable effects. The trust of individuals lessens if a system concerning the skill provides insufficient data. Consumers don’t need only the claims and assurances. They require the efficient results produced by the services for their benefits [4].

A. Control

For trust, power is quite a significant issue. If consumers don't have proper control over their assets, their confidence in the system will decrease. A usual example of control can be observed when individuals get the case from the ATM. They are assured that they will get the exact amount that they need. In other terms, they are controlling the money. The same opposite can be said when they are depositing. After all, they don't know just what will happen to their cash once they have collected it.

Similarly, if consumers have more control over the information delivered to the cloud, their trust in the cloud will increase [5].

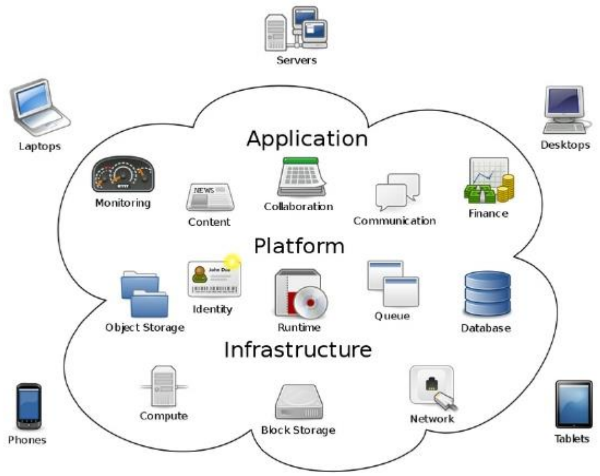

Fig.1 Cloud Computing [6]

B. Ownership

The variation of trust can also be observed relying on the purchase of assets that concern the data. For example, if an employer is trusting a service with the credit more, his trust will lessen when he has to believe it with the credit card of his employee as well. After all, it is his objective to preserve the confidence of an employee [7].

Similarly, firms or enterprises when consigning the information to the cloud, it represents not only the enterprise's interest but also the clients'. It will create a relationship with twofold and faces. First of all, the enterprise to trust the cloud service provider for itself.

Second, it must assure that the clients have almost the same reasons for believing the same service [4].

C. Prevention

For the establishment of trust, contractual relationships are mostly used. If the service is not offered according to the expectations, the firm will be compensated in a healthy environment of business. Similarly, the providers of cloud use the SLAs or service-level agreements to increase the trust of consumers. However, this might not be able to help in the case of cloud computing.

When it comes to trusting cloud computing, it is more like restricting a violation of trust rather than guaranteeing compensation in case of a breach. For many firms and enterprises, losing the data cannot be repaired. The extent of money cannot compensate for the precious information. The money can never improve Even the reputation. Therefore, the model of cloud computing should concentrate on preventing the failure rather than compensating [8].

D. Security

Guard plays the primary role in resisting a failure and nurturing trust in the methodologies of cloud computing. Notably, the protection of practical nature and environment must be provided by the providers of cloud service. After all, it allows them to perform actions and functions for various clients and provide individual services for several clients as well.

When it comes to virtualization, the main issues concerning the security are access control, data leakage, and persistent client-data security, and identity management, hindrance of attacks that concern the cross-VM side-channel, and VM protection or virtual machine protection. Whether the security risks are enormous or small, their presence threatens the trust of consumers. Therefore, it is essential to prepare and eliminate such risks rather than losing the confidence of consumers [1].

4. TRUST CHALLENGES

Say that there is a company named SoftCom, it handles digital images concerning the healthcare. These digital images are significant and confidential as well. Such vital data cannot be risked. The firm decides to use the public provided of cloud named CloudX. From the company, what would be the challenges?

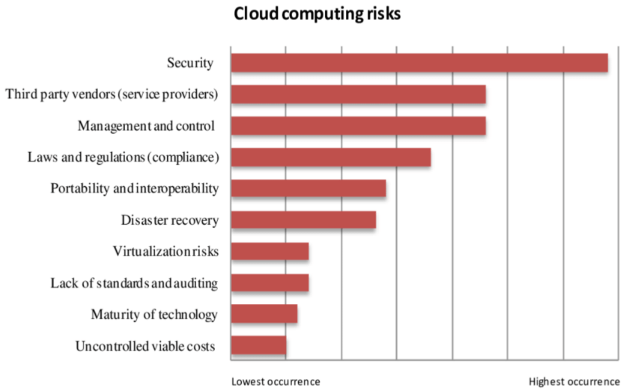

Fig. 2. Cloud computing risks [9]

A. Frail Control

SoftCom finds that once the images leave the boundary, they don't have much control over these images anymore. Even the processes are not under their control so they cannot manipulate these images anymore. The company doesn't know who is accessing the data and which party is handling it.

In the cloud computing, this risks of losing the information, its integrity, and its availability are quite threatening when it comes to the trust. Virtually, cloud computing requires the users to loosen their grip when it comes to storing the data.

The degree of losing the control over the processes and the data depend on the model of cloud service. Typically, enterprises have only partial control over the information which their find quite dangerous and alarming. After all, the data is precious and losing it cannot be afforded [10].

B. Lack of Confidentiality

Consumers think that a cloud is more threatening than a system in-house. However, improved secrecy in CloudX can help in covering the issue. The data in the cloud is not stored in a single device or a single location. It is actually processed and stored across the whole layer that is virtual. When it comes to the confidentiality, there are two issues. The first one involves the physical presence and location of processing and storage sites. The second is the secure identity or profiles of these locations or sites.

For the trust, an enterprise should know where and how the data is being processed. The security threats concerning the sites and quite high. After all, a company is accountable for the personal data of its clients [11].

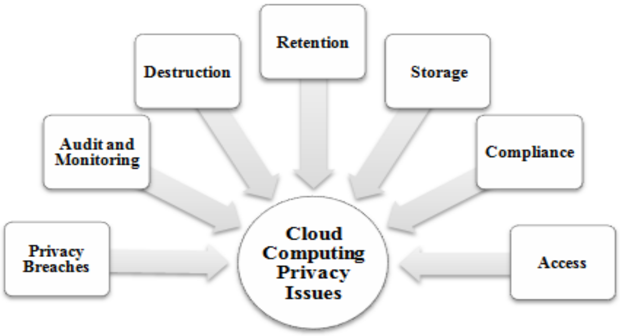

Fig. 3. Cloud computing security challenges [12]

5. HOW TO SOLVE THESE ISSUES?

Since the data of SoftCom is significant, it is essential for CloudX to:

- Notify SoftCom whenever someone accesses the data and the information that confidential.
- The data must be not be copied from the images unauthorized. To copy the data, it must the need the permission of SoftCom first.
- Destroy any residue that is not needed anymore. This way the confidentiality of the company will remain safe.

Organizations require additional assurances like:

- All applications must be reliable and must hold the data properly without damaging it at all. The processes must be trustworthy as well.
- The knowledge about physical location must also be spread to the company. This way it will know where the information is being stored.
- The security properties must be appropriately applied to the enterprise as well.

Sure, it will be daunting for the providers of cloud service. However, it is necessary for them if they want to actively build the consumer base [13].

6. CONCLUSIONS

Cloud computing delivers many new and efficient opportunities to enterprises. However, the risks and challenges threatening the trust of consumers are also present. For the service providers of the cloud to keep delivering successfully, they need to make sure that the enterprises have full control over the data. Some gaps are missing from the approach adopted by the cloud computing. Filling out these gaps requires the efforts. However, they ensure an efficient return from the consumers as well. The security and safety of data are critical. Most of the enterprises don't tolerate when it comes to these factors. That is why it is essential to focus on such points and build the trust of consumers. To develop the confidence, only the quality is not necessary. The security, confidentiality, and control are also important. With some more efforts, CloudX computing can secure a secure room in the functioning of enterprises [14].

REFERENCES

[1] S. Nepal, and M. Pathan, Security, Privacy and Trust in Cloud Systems, Springer Science & Business Media, 2013.

[2] M. A. Ahmad Ali, A. Khan, M. Ilyas, and M. S. Razzaq, "A Trust Management System Model for Cloud," IEEE, 2017.

[3] [3] P. Mell, and T. Grance, "The NIST definition of cloud computing.," NIST special publication, vol. 800, no. 145, p. 7, 2011.

[4] S. S. Kirkman, "A Data Movement Policy Framework for Improving Trust in the Cloud Using Smart Contracts and Blockchains," IEEE International Conference on Cloud Engineering, pp. 270-273, 2018.

[5] P. Manuel, "A trust model of cloud computing based on Quality of Service," Annals of Operations Research, 2013.

[6] Teoriasdadenny.com, "Imposing Architecture Cloud Computing," 2018. [Online]. Available: http://teoriasdadenny.com/imposing-architecture-cloud-computing/.

[7] M. K. Tripathi, and V. K. Sehga, "Establishing Trst in Cloud Computing Security with the Help of Inter-Clouds," IEEE, pp. 1749-1752, 2014.

[8] H. Krcmar, R. R. and, B. Rumpe, Trusted Cloud Computing, Springer, 2014.

[9] M. Carroll, A. V. D. Merwe and P. Kotze, "ecure cloud computing: Benefits, risks and controls," In Information Security South Africa (ISSA), pp. 1-9, 2011.

[10] T. Erl, R. Cope and, A. Naserpour, Cloud Computing Design Patterns, Prentice Hall, 2015.

[11] L.-q. Tian, C. Lin and, Y. Ni, "Evaluation of user behavior trust in cloud computing," In Computer Application and System Modeling (ICCASM), 2010 International Conference on, vol. 7, pp. V7-567, 2010.

[12] M. Alghali, N. H. M. Alwi and, R. Ismail, "Towards an Efficient Privacy in Cloud Based E-Learning," Data Mining and Information Technology, pp. 40-45, 2014.

[13] A. Barsoum and, A. Hasan, "Enabling dynamic data and indirect mutual trust for cloud computing storage systems.," IEEE transactions on parallel and distributed systems, vol. 24, no. 12, pp. 2375-2385, 2013.

[14] T. H. Noor, Q. Z. Sheng and, A. Bouguettaya, Trust Management in Cloud Services, Springer, 2014.